# Ambient Identity:

*Presence Without Surveillance*

Charles Magnarelli
Supah, Inc.
charlie@supah.dev

---

## Abstract

Every major technology platform is extending its identity model into physical space. Buildings unlock. Vehicles respond. Payments complete. Civic services recognize residents. The ambient intelligence layer is being built now, and the architecture chosen in this decade will determine whether the physical world becomes a domain of sovereign presence or total observation. We propose Ambient Identity (AI)—not artificial intelligence, but the extension of verified human identity into physical space through consent-based recognition. Building on Proof of Person (PoP), the Supah Identity Protocol (SIP), and the Ledgr custodial institution, Ambient Identity defines a framework in which sensors recognize only those who have authorized them to do so, within the precise scope of that authorization, with every interaction logged in an institution that cannot sell the record. The credential recognizes itself. The building doesn't remember the face.

---

## 1 Introduction: Two Futures

Ambient intelligence is coming regardless. The convergence of low-cost sensors, edge compute, and wireless mesh networking has made it technically and economically feasible to embed recognition capability into every doorframe, transit turnstile, hospital corridor, and public plaza. This transition is not contingent on any single company's roadmap. It is the product of compounding hardware economics and regulatory pressure for frictionless compliance. The question is not whether it happens. The question is on whose terms.

Today, three platforms are building the ambient layer. Apple is extending ambient intelligence through HomeKit, the Secure Enclave, and device-captive identity—a model in which the phone is the credential and the credential is indistinguishable from platform loyalty. Google is building it through Nest, Android, and behavioral inference—a model in which the ambient layer is a surface for the same advertising and prediction engine that has defined its internet presence for two decades. Amazon is building it through Sidewalk, Alexa, and its logistics network—a model in which ambient recognition is an extension of purchase history and delivery optimization.

Each of these architectures delivers real convenience. Each of them extends a surveillance model into physical space. The building that unlocks when your phone is near is also the building that

logs when you arrived, how long you stayed, and whether you came back. In the platform model, these logs belong to the infrastructure operator, the platform provider, and any third party to whom they are licensed. The resident is the subject of the record, not its owner.

There is a second future. In this future, sensors exist only in spaces you have explicitly authorized. Your credential presents itself through cryptographic handshake when you cross a threshold you have opted into. The infrastructure recognizes that a valid credential is present and responds accordingly—without storing a face, without building a behavioral profile, without informing any party beyond the one you granted permission to act. Outside of spaces you have authorized, you are invisible to the infrastructure. Not obscured. Not anonymized. Invisible, because no capture mechanism has been granted permission to see you.

These two futures produce identical user experiences. The door unlocks. The bus recognizes the pass. The hospital retrieves the record. The city issues the permit. The surface is the same. The architecture is opposite. Which architecture wins this decade determines whether ambient computing becomes the largest surveillance infrastructure in human history or the first physical extension of human digital sovereignty.

This paper argues for the second future and describes how to build it.

## 2 The Surveillance Model and Its Cost

To understand what the consent model prevents, it is necessary to describe the surveillance model with precision. The surveillance model has three defining characteristics.

**Continuous passive capture.** Surveillance-based ambient infrastructure operates by collecting from everyone and filtering for relevance afterward. A facial recognition system at a building entrance does not wait for residents to identify themselves—it photographs every person who approaches and runs recognition against a database. The people who are not residents are still photographed, still processed, still entered into the system as failed matches. The building accumulates a record of every face that passed its threshold, including people who never entered and never consented.

**Inference from observation.** Surveillance systems derive identity from behavioral patterns—gait, device proximity, facial geometry, habitual timing. The inference model depends on accumulation: each observation adds resolution to the behavioral profile, making recognition more reliable and the profile more valuable. There is no natural limit on collection because more data always improves the inference. The system has an architectural incentive to observe as much as possible.

**Operator-held records.** In a surveillance model, the log of what the system recognized belongs to whoever owns the infrastructure. A condo association that installs facial recognition owns the record of every resident's arrival and departure. A hospital that deploys behavioral monitoring owns the record of every patient's movement. A city that deploys smart surveillance owns the

record of every resident's presence in public space. The subject of the record has no claim on it. They cannot inspect it, correct it, revoke it, or know with certainty what was retained.

The costs of this architecture are not hypothetical. As documented publicly, facial recognition systems have been deployed in residential buildings in New York, Detroit, and Chicago over tenant objection. School districts in the United States have built student recognition databases that were later discovered to have been shared with law enforcement without parental consent. Municipal smart city deployments have accumulated movement records that proved legally discoverable in civil litigation against the very residents whose convenience they were designed to serve.

The convenience of surveillance-based ambient intelligence is genuine. The cost is that presence in any space that has deployed the infrastructure is no longer private. It is observed, recorded, and held by an entity whose interests may not align with yours.

This outcome is not what the researchers who imagined ambient computing had in mind. Mark Weiser, working at Xerox PARC in the early 1990s, described a future of ubiquitous computing in which technology disappears into the environment—present everywhere, demanding attention nowhere. The most profound technologies, he wrote, are those that weave themselves into the fabric of everyday life until they are indistinguishable from it [11]. The surveillance model is the inversion of that vision: technology that is present everywhere and demands attention constantly, not by notifying you, but by watching you. Weiser's ambient computing was designed to serve the human without interrupting them. The surveillance model serves the operator at the cost of observing everyone.

## 3 Ambient Identity: A Definition

In 2026, every technology company is racing to build AI. Supah is building AI too—not artificial intelligence, but Ambient Identity: the extension of verified human personhood into physical space through consent-based recognition.

The reclamation is deliberate. Artificial intelligence describes what machines do with data they have collected about you. Ambient Identity describes what happens when you bring your own verified credential into a space, present it on your terms, and withdraw it when you leave. One model optimizes the machine's knowledge of the human. The other extends the human's sovereignty into the machine's domain.

Ambient Identity is defined by four principles.

**Presence requires permission.** A space may recognize a verified human identity only if that individual has explicitly granted it permission to do so. The default state is invisibility. There is no passive enrollment, no ambient collection, no recognition of unconsenting individuals.

**Recognition is scoped.** Every grant defines precisely what the infrastructure may recognize, under what circumstances, and for what purpose. A grant to a building's front door is not a grant to the building's elevator, parking garage, or fitness center. Each context requires its own authorization. The scope is set by the user, not the infrastructure operator.

**The credential recognizes itself.** Recognition does not require a database of faces, behavioral profiles, or persistent identifiers. The user's credential—resident in the secure element of their phone or card—engages in a cryptographic handshake with authorized infrastructure and asserts its own validity. The sensor does not reach into a database to find you. You present yourself, within the scope of what you have permitted.

**The record belongs to you.** Every ambient interaction is logged in Ledgr, an independent 501(c)(3) nonprofit custodian whose charter prohibits the sale of data. The operator of the infrastructure cannot hide from you what it recognized. The history of your presence across every space you have authorized is visible to you through supah.id. You own the record of your own presence.

These four principles have an intellectual antecedent. The Calm Tech Institute, building on Weiser's Xerox PARC research, has formalized the design philosophy of ambient computing into the Principles of Calm Technology: that well-designed ambient systems should require the smallest possible amount of attention, make use of the periphery rather than the foreground, communicate without demanding acknowledgment, and respect social norms [12]. Consent-based ambient infrastructure satisfies these principles structurally. A proximity handshake that unlocks a door without requiring the resident to take out their phone, enter a code, or be photographed is, by definition, calm. Surveillance infrastructure violates them architecturally. A system that photographs everyone who approaches regardless of their intent, runs their face against a database, and retains the result is not operating at the periphery of anyone's attention. It is extracting from it. The distinction between these two architectures is not a matter of implementation quality. It is a matter of design commitment.

## 4 The Architecture of Consent

The technical foundation of Ambient Identity is the sovereignty stack described in Proof of Person and Supah 2030: Proof of Person (PoP) for verified credential issuance, the Supah Identity Protocol (SIP) for consent-based data exchange, and Ledgr for independent custodial preservation. Ambient Identity extends this stack from online interactions into physical space through five mechanisms.

### *4.1 Ambient Grants*

An Ambient Grant is a permission issued by a user to a specific space, device, or district, defining what the infrastructure is authorized to recognize and for what purpose. Grants are

issued through supah.id and stored in the user's credential. They are precise, bounded, and revocable.

A grant is not a blanket authorization. It specifies the counterparty (this building, this hospital system, this transit network), the context (front door, medication dispensary, fare gate), the time bounds (business hours, indefinite, event-specific), and the permitted action (unlock, access, authenticate). Infrastructure that exceeds the scope of a grant receives no response from the credential.

The grant model inverts the current architecture. Today, infrastructure is deployed and users are enrolled. Under Ambient Identity, the user issues the grant and the infrastructure operates within it. Consent precedes capability.

### *4.2 Proximity Handshakes*

Recognition in the Ambient Identity model does not involve databases of faces, behavioral signatures, or passive radio scanning. It involves a cryptographic challenge-response between the user's device and authorized infrastructure.

When a credential holder approaches an opted-in threshold, their device broadcasts a cryptographic token derived from their SPN—the Supah Person Number resident in the device's secure element—in a form specific to the granted context. The infrastructure presents a challenge. The device answers with a proof that is valid only for this grant, at this time, in this context. The infrastructure cannot derive the underlying SPN from the token. It cannot share the token with another system and receive the same proof. Each handshake is context-specific and non-transferable.

The sensor does not identify you. It confirms that a credential is present that has authorized this recognition event. The building doesn't remember the face. It records that a valid grant was exercised at a specific time, by an anonymized grant identifier, for a specific permitted action.

### *4.3 Scoped Recognition*

The principle that recognition is bounded by grant scope has a corollary: a grant in one context produces no recognition in any other context. A grant to your employer's building does not grant recognition to the coffee shop in the lobby. A grant to a hospital system does not grant recognition to the pharmacy across the street, even if the pharmacy is affiliated with the same health network. Each context is independent.

This is the architectural inverse of platform identity. Apple's ambient intelligence layer recognizes you across every HomeKit-enabled space, every iOS device, and every service integrated with the Apple ecosystem, because your identity is captive to the platform that follows you everywhere. SIP-based Ambient Identity produces recognition only where you have chosen to be recognized. Outside of those spaces, you are not anonymized. You are absent. The

infrastructure has no token to match and no behavioral signal to infer from, because none was ever offered.

### *4.4 The Log, Not the Feed*

Every ambient interaction produces an entry in Ledgr: grant identifier, timestamp, counterparty identifier, permitted action, outcome. The entry is append-only. It cannot be deleted, modified, or withheld from the user who generated it.

This is the institutional distinction that makes Ambient Identity structurally different from privacy-preserving alternatives that rely on technical obfuscation. Zero-knowledge proofs and differential privacy protect data in transit and in computation. Ledgr protects the record of what happened over time, in an institution whose governing documents prohibit its commercialization.

When a user reviews their ambient history on supah.id, they are querying their own Ledgr record. When a civil liberties organization audits a municipality's ambient deployment, it is examining Ledgr logs. When a dispute arises about whether infrastructure had authorization to recognize a credential, the record in Ledgr is the authoritative source. The log is not a surveillance feed. It is the user's audit trail of their own sovereign presence.

### *4.5 Revocation*

Any Ambient Grant can be revoked at any time through supah.id. Revocation propagates immediately to the counterparty infrastructure. The next handshake attempt by that infrastructure receives no response from the credential. Effective recognition capability ends at the moment of revocation.

This capability—instant, user-initiated revocation of physical recognition—does not exist in current ambient systems. A resident who wants to stop a platform-based smart lock from recognizing them must replace the hardware, leave the platform, or petition the building management. Under Ambient Identity, the user withdraws the grant and the infrastructure loses access. The power relationship is reversed.

## 5 Powered by Supah: The Trust Mark

A building, hospital, school, or city that deploys Ambient Identity infrastructure on the SIP protocol is making a verifiable commitment: we operate consent-based recognition infrastructure. We do not surveil people who enter our spaces. We recognize only those who have granted us permission to do so, within the scope they defined.

This commitment is signaled publicly through the "Powered by Supah" mark—a trust mark for ambient computing infrastructure. A space that displays the mark is declaring that its recognition systems operate on the Ambient Identity architecture: no passive collection of unconsenting

individuals, no behavioral inference, no operator-held face databases, all interactions logged in an independent custodian accessible to the individuals involved.

The mark will become, over the course of this decade, what organic certification and LEED ratings are today: a public signal that the infrastructure here operates on an ethical architecture. The signal is not primarily a marketing claim. It is a legal and technical commitment backed by the SIP protocol itself, which enforces scope constraints at the infrastructure layer. A "Powered by Supah" building cannot exceed the scope of issued grants without generating protocol violations visible in Ledgr—violations that are discoverable by the user whose grant was exceeded.

Infrastructure operators will adopt the mark for four reasons.

**Differentiation.** Surveillance fatigue among tenants, employees, patients, and residents is documented and growing. The "Powered by Supah" mark is a competitive differentiator for building owners, employers, healthcare systems, and municipalities that want to attract privacy-conscious occupants and citizens.

**Liability reduction.** An infrastructure that cannot retain a facial recognition database cannot be compelled to produce one in litigation, cannot be breached in a way that exposes it, and cannot be the subject of regulatory action premised on unauthorized data collection. The system is incapable of the violations that generate liability, because it never creates the asset that becomes the liability.

**Regulatory alignment.** State biometric privacy laws, including Illinois BIPA and the growing class of state-level equivalents, impose significant liability on operators of facial recognition and behavioral surveillance systems. GDPR and its international equivalents impose data minimization requirements that consent-based recognition satisfies by design. The "Powered by Supah" architecture is not merely compliant with these frameworks. It is compliant by construction—structurally incapable of the practices the regulations prohibit.

**Trust compounding.** A building that operates on Ambient Identity for five years has a Ledgr record demonstrating five years of compliant, consent-based recognition. That record is auditable. It creates a form of institutional reputation that surveillance-based infrastructure cannot generate, because the logs it holds are proprietary and unverifiable by the occupants they concern.

The precedent for domain-specific trust marks in ambient technology already exists. The Calm Tech Institute has established Calm Tech Certified™, an 81-point evaluation framework that certifies products for their attention-aware design properties—assessing periphery engagement, tactility, material use, and the degree to which a product works with human attention rather than against it [12]. The certification has been adopted by manufacturers ranging from enterprise computing to smart home hardware. It demonstrates that operators and manufacturers will seek and display marks that signal ethical design commitments, when those marks carry real technical

content. The “Powered by Supah” mark operates on the same institutional logic in the ambient identity domain: not a self-reported claim, but a verifiable commitment backed by the protocol itself.

## 6 Examples in the Wild

The following examples describe the same user experience under surveillance architecture and under consent architecture. The experience is identical. The infrastructure is opposite.

### *6.1 The Building Door*

A residential building on surveillance architecture installs a camera at the entrance and runs facial recognition against an enrollment database built from resident photographs submitted at move-in. Every person who approaches the building is photographed. Non-residents are logged as non-matches. Residents are recognized and the door unlocks. The building operator retains a timestamp-indexed photographic record of every person who approached the entrance.

A residential building “Powered by Supah” has a proximity reader at the entrance. Residents issue an Ambient Grant to the building system authorizing credential recognition at the front door between their chosen access hours. When a resident approaches, their device executes a handshake with the reader. The door unlocks. No photograph is taken. No database of faces exists. Non-residents who approach the building generate no record because they have no credential registered with that infrastructure. The credential recognizes itself.

Both doors unlock when residents arrive. One building watches everyone who passes. The other sees only those who have chosen to be seen.

### *6.2 The Hospital Record System*

A hospital operating on surveillance architecture builds a patient data repository that logs every chart access, every medication dispense, every room entry. The data is accessed through institutional credentials managed by the hospital’s IT department. The patient’s record exists in a database the hospital controls, which becomes the target for the breach events that have exposed hundreds of millions of Americans’ health records in the past decade.

A hospital “Powered by Supah” accesses patient data through SIP consent flows tied to the patient’s PoP credential. The patient has issued a scoped grant to the hospital system authorizing access to specific record categories. Each access request executes a SIP transaction logged in Ledgr. The patient can review, at any time, which provider accessed which data category and when. The record is not retained in a hospital database in the form that constitutes a breach target—it is transmitted per-request, within the scope of the active grant, and the log is held by the custodian the hospital cannot control.

The convenience is identical. The breach surface is gone.

### *6.3 The School District*

A school district deploying surveillance-based attendance infrastructure builds a facial recognition database of every enrolled student. This database—containing biometric identifiers for minors—becomes an institutional asset, a legal liability, and a target. As documented in publicly reported cases, school biometric databases have been shared with law enforcement agencies without parental notification, subpoenaed in civil proceedings, and exposed in breach events that parents had no means to prevent or remedy.

A school district "Powered by Supah" issues credential grants to enrolled students and their guardians. Attendance is confirmed through proximity handshakes at classroom thresholds. The system confirms that an authorized credential is present without building a biometric database of student faces. The school can prove attendance with the same reliability as facial recognition. It does not create the database that becomes the liability.

No face is remembered. Attendance is proven. The students leave no biometric record at the institution.

### *6.4 The Municipal Civic Experience*

A city deploying smart city infrastructure through surveillance architecture builds a network of sensors that can confirm residents' identities for civic services—automatic parking payment, public building access, event credentialing, transit fare management—by maintaining a persistent record of residents' movements through public and semi-public space. The convenience is real. So is the archive of municipal observation.

A city "Powered by Supah" deploys SIP-enabled kiosks at opted-in locations. Residents who choose to participate issue Ambient Grants to specific municipal services. Transit fare gates recognize credentials that have granted them access. Permit kiosks authenticate identity through handshake for document retrieval. Parking meters settle payment through the SupahCard credential without transmitting location data to a central database.

The resident experiences frictionless civic interaction. The city does not accumulate a surveillance record of who went where and when. The service operates. The observation does not.

## 7 Why Existing Approaches Fail

The consent-based ambient intelligence model is not a new idea. It has been proposed, implicitly or explicitly, in several prior architectures. None of them succeed for reasons that are structural, not technical.

**Device-captive identity (Apple, Google).** Platform ambient identity systems work only within the ecosystem. The credential is not portable between platforms. More importantly, the

credential cannot be revoked without losing the platform relationship—you cannot withdraw recognition capability without leaving the ecosystem. And the log of recognition events belongs to the platform. These systems solve the recognition problem while preserving the platform's position as the entity that holds the ambient record and controls the credential's scope.

**Federated identity (OAuth, SAML).** Federated identity systems delegate trust to intermediaries—platforms that issue tokens on behalf of users and broker identity claims to third parties. The intermediary becomes a single point of failure and commercial capture. The grant model in federated identity is controlled by the identity provider, not the user. And federated systems were designed for web authentication, not physical-space recognition—extending them into ambient computing replicates the platform-captive problem in a different form.

**Decentralized identity (DID, Soulbound Tokens).** Decentralized identity proposals correctly identified the sovereignty problem in platform-captive systems and proposed cryptographic primitives as the alternative. The proposals fail on institutional grounds. A cryptographic proof that a wallet controls a key does not answer the question "is this a real person?" It answers the question "does this entity control this key?"—which is authentication, not verification. Without the institutional verification that Proof of Person provides, decentralized identity has no answer to Sybil attacks, synthetic identities, or real-world compliance requirements.

**Government digital ID (eID, REAL ID, national digital identity schemes).** Government-issued digital identity solves the verification problem but introduces a different set of constraints. Government identity is captive to the issuing state, rarely ports across jurisdictions without friction, and is politically fragile: a change of administration can alter the surveillance posture of the identity system overnight. In several documented cases, government digital identity programs have been designed with ambient surveillance as a feature, not a limitation.

Supah's Ambient Identity is the only proposal that provides all four components simultaneously: verified personhood through PoP, portable and user-owned credential through the SPN, protocol-level consent through SIP extended into physical space, and institutional independence through Ledgr. No single component is novel. The architecture that puts them together in a user-sovereign system is.

## 8 The Role of the Custodian

In a surveillance-based ambient system, the log of your presence belongs to whoever owns the infrastructure. In the Ambient Identity model, the log belongs to you—and the institution that holds it cannot sell it.

Ledgr is a 501(c)(3) nonprofit with a charter that prohibits the sale of identity metadata. It is governed by an independent board with no Supah executives. It stores not personal data but the audit record of consent: which grants were issued, which recognition events occurred, what was authorized and when. The log is append-only. Entries cannot be deleted.

This is not a technical distinction. It is an institutional one. The question of who holds the record—and under what governance—is a more durable form of privacy protection than any encryption scheme or access control system. Encryption can be broken. Access controls can be changed by a new owner. But an independent nonprofit with a structurally enforced prohibition on data commercialization, modeled on the relationship between a central bank and its regulated institutions, creates a form of institutional accountability that technical controls alone cannot replicate.

When a user reviews their ambient history on supah.id, they are querying their own Ledgr record through SIP—the same protocol that any third-party organization would use. Supah, Inc. does not hold a privileged access path to Ledgr. The nonprofit's independence ensures that no future executive of the commercial company can liquidate the custodial record for revenue. Capital never flows from Ledgr to Supah.

When a dispute arises about whether a space exceeded the scope of an Ambient Grant, the record in Ledgr is authoritative. When a civil liberties organization requests an audit of a municipality's use of recognition infrastructure, the evidence is in Ledgr. When a user moves cities, changes employers, or withdraws from a space, the history of their presence there remains in the custodian they control, not in the operator they left.

The custodian is the difference between ambient sovereignty and ambient surveillance. The architecture of Ambient Identity could be technically correct and institutionally hollow—if the log were held by the operator, or by Supah, or by a nonprofit that could be dissolved or acquired, the consent model would be a surface over the same underlying surveillance structure. Ledgr is the institutional guarantee that the consent model is real.

The governance problem that Ledgr solves has a precise analog in the digital domain. The Metagovernance Project—a nonprofit laboratory for digital governance founded out of Harvard Law School and the MIT Media Lab—has described the internet's governance challenge as requiring a layer that governs not just individual communities or platforms, but the interaction between them [13]. Their framing of metagovernance as governing the interaction between separate institutions describes exactly the custodial problem in ambient infrastructure. Each building, hospital, school, and city that deploys SIP-based recognition is a separate institution operating on the same identity protocol. The question of who audits the auditors—who ensures that each operator stays within its granted scope, and who holds the record when disputes arise between institutions—is a metagovernance question. Ledgr is the custodial institution that answers it: a governance layer for ambient recognition infrastructure that is, in Metagov's words, empowering, accountable, and structurally independent of the institutions it governs.

## 9 The Window

The window to build consent-based ambient infrastructure is finite, and it is open now.

Physical ambient infrastructure is expensive and slow to deploy. Cameras, proximity readers, mesh network nodes, and edge compute are installed in buildings and transit systems on multi-year timescales. The upgrade cycles are long. Once a building installs facial recognition infrastructure—the cameras, the database, the enrollment workflow—the switching cost to a consent-based alternative rises substantially. The organization has a sunk investment in surveillance infrastructure and an existing data asset that the consent model explicitly prohibits.

Once every building in a city has facial recognition at its entrance, the technical argument for a consent-based alternative is correct but the economic argument is hard. The ambient surveillance layer will have been built. Retrofitting it requires replacement, not upgrade, because the architectural difference between surveillance recognition and consent recognition is not a software parameter. It is the presence or absence of a face database, which the consent model requires not to exist.

The window is open because the deployment has not yet reached critical mass. Smart locks, proximity readers, and credential-based access systems are in the market and growing. Facial recognition at scale in residential and commercial buildings is documented in major urban centers but not yet universal. Transit systems are deploying biometric fare payment but the standards are not locked. Healthcare access management is modernizing but not yet consolidated around any single vendor.

The standards set now will determine which architecture those deployments use. If the first generation of frictionless building access is credential-based, the infrastructure is Ambient Identity-compatible. If it is face-database-based, the installed base will resist migration. Infrastructure incumbency is real.

Supah is the only entity currently in the market with the complete stack to build the consent-based alternative: verified personhood through PoP, portable credential through SPN, consent protocol through SIP, physical infrastructure through Supah Compute, and independent custody through Ledgr. No incumbent technology platform can build this architecture for the same reason no incumbent can build the open identity layer: their business model depends on the data that the consent model requires not to collect.

The argument for the surveillance model is not that it is better. It is that it is already being built. The argument for the consent model is not that it is more sophisticated. It is that it is the only version of ambient intelligence worth building—and the time to build it is before the other version is everywhere.

## 10 Conclusion

Ambient intelligence will extend the internet into physical space. Sensors will recognize the people who have granted them permission. Infrastructure will respond to presence. Civic services

will be frictionless. The question this paper has argued is not whether this happens but whether presence requires observation.

The surveillance model answers: yes. You must be watched to be served. Your face must be in a database. Your movements must be logged by the operator. Your patterns must be available for inference. The convenience is real. The cost is the end of the private moment in any space that has deployed the infrastructure.

The consent model answers: no. You may be recognized without being watched. The credential recognizes itself. The building doesn't remember the face. The infrastructure responds to your presence without accumulating the evidence of it. Every recognition event is logged in an institution you own the record of, not one that owns the record of you.

These are not two points on a privacy spectrum. They are two different architectural commitments about the relationship between human beings and the systems that serve them. Ambient Identity is the technical and institutional infrastructure that makes the consent model real, scalable, and durable.

Presence without surveillance is not a feature. It is the founding principle of a built environment worth living in.

---

## References


[1] C. Magnarelli, "Proof of Person: A Sovereign Verification Protocol for Human Identity," Supah, Inc., April 2026.

[2] C. Magnarelli, "Supah 2030: Identity Infrastructure for the Verified Internet," Supah, Inc., April 2026.

[3] Apple Inc., "HomeKit and Matter: Smart home protocol documentation," developer.apple.com, 2024.

[4] Amazon, "Amazon Sidewalk: Network architecture and device specifications," developer.amazon.com, 2024.

[5] T. Wu, The Attention Merchants: The Epic Scramble to Get Inside Our Heads, Knopf, 2016.

[6] Georgetown Law Center on Privacy and Technology, "America Under Watch: Face Surveillance in the United States," 2022.

[7] Electronic Frontier Foundation, "The Secretive Company That Might End Privacy as We Know It," EFF.org, updated reporting 2023–2024.

[8] Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14 (2008). See also: Texas CUBI, Washington MY Health MY Data Act, and state-level equivalents enacted through 2025.

[9] European Parliament, "Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act)," Official Journal of the European Union, June 2024.

[10] B. Schneier, Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World, W.W. Norton, 2018.

[11] M. Weiser, "The Computer for the 21st Century," Scientific American, vol. 265, no. 3, 1991. See also: M. Weiser and J.S. Brown, "Designing Calm Technology," PowerGrid Journal, 1996.

[12] A. Case, Calm Technology: Principles and Patterns for Non-Intrusive Design, O'Reilly Media, 2015. See also: Calm Tech Institute, "Principles of Calm Technology," calmtech.institute, 2024–2026.

[13] Metagov, “About Metagov: A Laboratory for Digital Governance,” metagov.org, 2020–2026. See also: J. Tan et al., “Governance of Online Communities,” Metagovernance Project, 2019–2024.

supah.dev • charlie@supah.dev