

Recognition Without Surveillance

Personalization as a local property: how a home can know its family without a profile ever leaving the house.

Pieter Meyer · Elysium Labs · Zürich, Switzerland

ELY-TR-2026-03 · Version 1.3 · First published 12 July 2026 · Revised 11 October 2026

Self-published technical report · not peer reviewed

Abstract

A home that serves the people in it has to know them: who is acting, whose morning routine this is, which requests come from the twelve-year-old, and which requests are standing preferences and which are one-time commands. In the dominant commercial pattern, knowing the resident means assembling a profile of them in a datacenter, where it can be retained, correlated across services, and monetized. Personalization and surveillance become the same act, and the resident is asked to accept the second to get the first. This paper describes an architecture in which recognition, and the memory it produces, belong to the home. In the Sovereign placement, which is how the hub ships, the household model, the standing preferences (one active value for each room, setting and occasion, with authorship recorded) and the memory of what the home has learned are stored and processed on the hub and do not leave the house. In the Hybrid placement they are stored only on the hub, and the parts relevant to a request travel with it to the reasoning model, as our companion report's disclosure lists [8]. Here we apply to what the home learns about its people the same placement that report applies to inference. On that foundation the design makes three commitments. Enrollment is a mutual, revocable act: a person is added to the household deliberately and can be removed at will. The system optimizes for discretion: each person gets the reach in the house that fits them, and a guest gets what their pass names and none of the household's memories, preferences, calendar or settings. And what the home knows about each person is legible to that person and erasable on request. We describe the access model the product enforces today, list what the home keeps about each person and how each item is removed, state which recognition signals are operational and which belong to a later hardware phase, and close with the limits we consider intrinsic.

1. The personalization dilemma

A useful home assistant is personal by necessity. A shared, anonymous device can turn on a light, but it cannot know that "my usual" means the bedroom at 21 degrees, that the child's tablet should go quiet at nine, or which requests come from a resident with broad reach in the house and which from a guest who

should get the lights and nothing more. Every capability that feels like care depends on the home knowing who it is serving.

The most common design builds that model on the vendor's servers. Amazon's voice profiles, which tell household members apart, depend on voice recordings saved to Amazon's cloud and stop working when a user chooses not to save them [11]. Local designs exist: Apple's HomeKit Secure Video analyzes camera frames on a home hub in the house [12]. What remains uncommon is keeping the whole household model, including the assistant's memory of each person, on hardware the household controls and can check.

Studies of smart-home users find that whether a flow of household information is acceptable depends on who receives it and for what purpose [6, 7]. Contextual integrity [1] gives that finding a precise form: information flows carry norms tied to the context in which they occur, and a flow, including a collection, violates privacy when it breaks those norms, for example by moving information to a party or a purpose the context did not sanction. A household butler who keeps the family calendar acts within the norms of the home, and passing that calendar to an advertiser would break them. We use that distinction as the design specification for the rest of this report.

2. Recognition as a local property

The Sovereign placement described in our companion report keeps inference, identity and memory on a single machine on the home network, and holds a hard rule that the hub sends no raw audio or video out of the house [8]. The people in the household, their names, their standing preferences and the assistant's memory of what it has learned are stored on the hub. Placement decides who else reads them. In Sovereign, only the software on the hub does, and the hub sends nothing about the resident out of the house unless the household turns on one of the kinds of egress our companion report lists, such as web search [8]. In Hybrid, a request sent to a cloud model carries the context it needs: the recent conversation, the memories chosen for it, the rooms and devices with their current state, the house instructions the household has set, and the resident's display name, preferred reply style and, if they wrote one, the short description in their profile. Elysium keeps no profile in the datacenter, and the hub lists what crosses, category by category [8]. In Cloud, the hosted deployment for households without a capable hub, the household model lives in Elysium's cloud account.

This inverts the usual data flow. In the cloud pattern, the signal (a voice, a face, a routine) travels to the model, and a profile accumulates far from the person. In the Sovereign placement the model is already where the person is, so the signal stays home and no external profile exists to accumulate. Figure 1 contrasts the cloud pattern with the Hybrid and Sovereign placements.

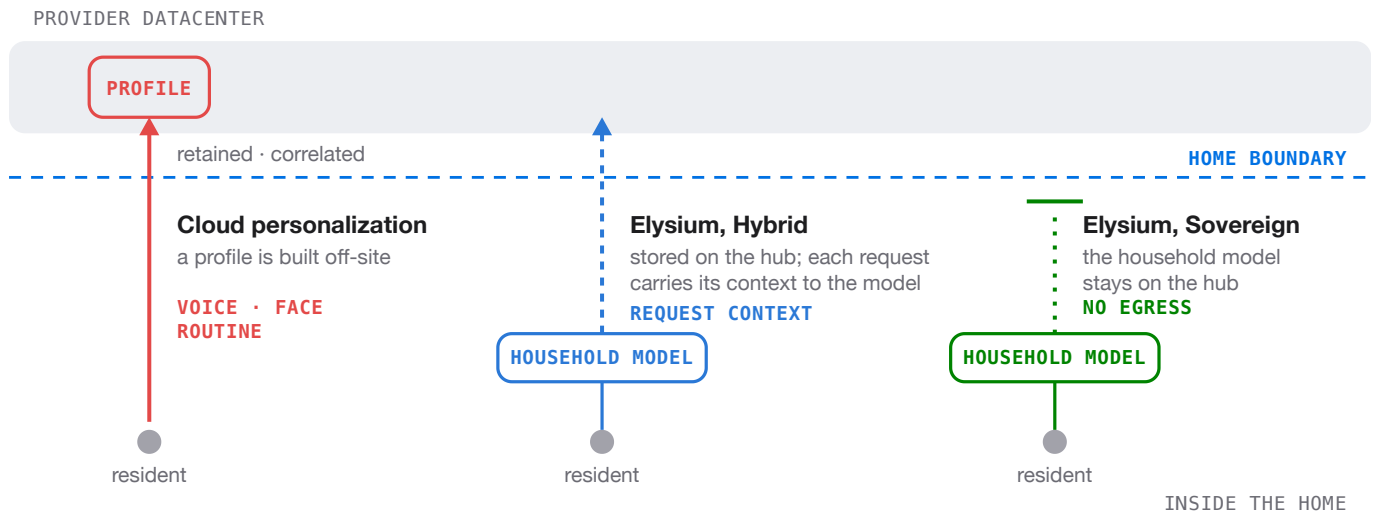


Figure 1. Where a home's knowledge of its people lives. In the cloud pattern, signals leave the house and a durable profile accumulates in a provider datacenter. In Elysium's Sovereign placement that knowledge (the household model, the preferences and the memory) lives on the hub inside the home and does not leave it. In Hybrid it is stored on the hub, and the context relevant to each request travels with that request to the reasoning model.

The privacy of personalization is therefore settled by where the data is. A profile that is never assembled outside the house cannot be breached there, combined with a shopping history or put to a purpose the household never agreed to. In the terms of Solove's taxonomy of privacy, these are the harms of insecurity, aggregation and secondary use [2]. In the Sovereign placement the owner can check this directly with the egress test described in the companion report [8].

3. Enrollment is mutual and revocable

Covert recognition is the default that makes people uneasy: a camera that silently learns the faces of everyone who passes is building a record no one consented to. Elysium treats enrollment as an explicit, mutual act (Figure 2). A person is added to the household by invitation, its adult residents can see who is enrolled, and any enrollment can be undone.

Making enrollment first-class has two consequences. Consent is legible: being recognized by the home is something a resident opted into and can point to. And standing is reversible. Removing a person ends their standing at once: their sessions and the scheduled tasks they created end, and their standing preferences are retired and their personal memories erased unless the administrator who removes them chooses to keep either. What they added for the whole household, such as shared memories, scenes and automations, stays with the household. A guest pass expires on its own, and guest conversations are not mined for memories. The design goal is that no one is recognized by the home without having chosen to be, and that the choice can be withdrawn as easily as it was made.

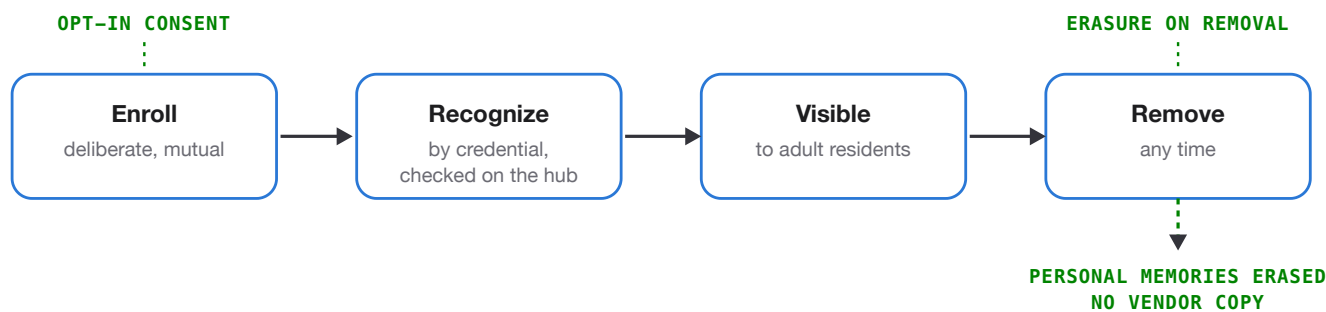


Figure 2. The enrollment lifecycle in the Sovereign placement. A person is added deliberately, identified only by credentials the hub checks, visible to the household's adult residents while enrolled, and removable at any time. Removal ends their standing at once and, unless the administrator chooses otherwise, retires their standing preferences and erases their personal memories.

4. Discretion over identification

A recognition system can be built for maximal identification, knowing exactly who everyone is. What a household wants is discretion, the appropriate matching of access to person, and discretion needs far less certainty than identification does. Our working model is the household butler, who serves each person according to their standing in the house.

The product enforces this as tiered access. A resident has broad reach across the home. A child has a reduced set of actions: lights, saved scenes, their own reminders, status reads and web search, without direct climate control or standing settings, although a saved scene can include a thermostat setting. A guest is granted the device types their pass names, and anything outside it is declined openly: when a guest asks for something they were not given, the assistant says so plainly and does not perform it, which keeps the boundary observable to everyone in the room. Table 1 shows the shape of the ladder.

Table 1. Access tiers as the product enforces them.

ACCESS TIER	REACH	MEMORY	EXAMPLE
Resident (admin or member)	Every room and capability; admins also manage the roster and guest passes	Their own personal memory and the shared household memory	"Set the bedroom to 21 and remember it."
Child	Lights in any room, saved scenes, their own reminders, status reads and web search; no direct climate control, automations or standing preferences, and a child's instruction applies once	Their own personal memory; can read the shared household memory but not change it	"Turn my lights down."
Guest (PIN pass, 1 hour to 30 days)	Only the device types the pass names, in any room	None; guest conversations are not mined for memories	"Turn on the living-room lights." Done. "Remember that I like it warm." Declined in the reply.
Shared wall panel, nobody identified	The guest set of actions	Household memory only, until a resident identifies with name and PIN	"Lights on in the kitchen."

A guest pass names the device types it covers. When a guest asks for a device type the pass does not name, the tool is not run, and the refusal returns to the assistant as a fixed result that it is told to relay, so the guest hears what the pass covers. Tools reserved for residents are not offered in a guest session at all, and a call that names one anyway is refused the same way. A guest session also cannot read the household's memories, preferences, calendar or settings through any interface, and it is kept off the live device-state channel that residents' dashboards use. The access model defines and enforces these tiers in code, and a resident's role is set when they accept an invitation. The household simulator described in our second report [9] has a guest probe that is run by hand; its nightly runs do not include it. The probe signs in with a guest pass and reports a failure if a tool reserved for residents runs in that session. Since October 2026 it also requests the household's memories, standing preferences, settings and calendar with the guest's pass and reports a failure if any of them is returned. When it was run against the product's code on 10 October 2026, every one of those requests was refused.

5. What is recognized, and what it is for

Recognition in the home serves two ends: routing a request to the right person's access and preferences, and keeping continuity across days so a resident is not made to repeat themselves. The clearest form of continuity is the standing preference. A resident states a preference once, "keep the bedroom at 21 degrees," and the home holds it and re-applies it without being asked again, through the same local device control the hub uses for every command [10]. In the current version a temperature preference is re-asserted whenever the thermostat reports a value more than 1.0 °C from the stated one, and a brightness preference is re-applied on the room's occupancy reports when a light is more than 10 percentage points off. A standing preference is a household rule: for each room, setting and occasion (always, in the evening, or on entering the room) the home keeps one active value and records who set it, and when a new preference from one resident displaces another's, it says so openly.

The way the home tells people apart is chosen to be the least invasive that will do the job, and today that is a credential. A resident is known by their sign-in, a guest by a short code that expires, and a person at a shared wall panel by tapping their name and entering a personal PIN. No biometric is read. Voice follows the same rule. The decision that speech is addressed to the assistant is made on the device, speech that is not addressed to it is discarded there, and in Sovereign what a person says to the hub becomes text on the hub, so the audio never leaves it. In Hybrid an owner can turn on a cloud recognizer for requests addressed to the assistant, cloud follow-up detection, which checks what the hub hears in the seconds after a reply, and a fast cloud model that tries to answer spoken requests first; the hub lists each [8]. Recognizing a specific person by their voice is a later phase, and it will be treated as a low-assurance signal for discretion that never substitutes for a credential [3, 4, 5].

Today the household model, the tiered access and the household's standing preferences are exercised through the assistant's text interface and the household's dashboard, with identity established by credential. Voice is in active hardware integration and is designed to feed the same access and preference machinery.

6. Legible and erasable

A home that knows its family should be able to say what it knows and to forget on request. Residents can see the standing preferences the home holds and the memory it has formed, and each of these can be removed. Memory is scoped: what a resident tells the home in confidence is kept as their own memory, which no one else in the household can open in the app, while what belongs to the home as a whole is shared, so discretion holds among residents in the app as well as against the outside world. Table 2 lists what the home keeps about a person, who can read it in the app and how each item is removed, and the paragraph after it describes the backups that reach further.

Table 2. What the home keeps about a person, who can read it in the app, and how it is removed.

ITEM	WHO CAN READ IT IN THE APP	HOW IT IS REMOVED
Personal memories	The person; an administrator's backup of the household holds their words, without saying whose they are	Forgotten one at a time, with everything else on request, by default with the person's removal, or with their account
Household memories	Every resident, children read only; the assistant also draws on them for anyone at a shared wall panel	Forgotten by the resident who added it or by an administrator, or deleted with the account of the resident who added it
Standing preferences	Every resident	Removed by any adult resident (an administrator's only by an administrator), retired by default with the person who set them, or deleted with their account
Conversations and messages	The person	Deleted one at a time, with everything else on request, or with the account
What they said at a shared wall panel	Adult residents, and anyone at that panel the same day	With everything else on request, or with the account
The words of spoken requests	The person whose conversation holds them; others see only timings	With the conversation, on request, with the account, or automatically after 14 days by default

Backups reach further than the app. An administrator can download a backup of the household from the dashboard. It holds the household's memories, standing preferences, settings, automations and scenes, and the words of every resident's personal memories without saying whose they are; it leaves out conversations, messages and the words of spoken requests. The hub's own backups, which the owner makes on the hub or turns on to run nightly, copy its whole database, so whoever holds one can read every item in Table 2.

Forgetting erases. When a memory is forgotten, its words, its search representation and every earlier version it replaced are wiped on the hub in the same step. A record without the text remains: who added the memory, whether it was personal or shared, its broad category, when it was made, and when and how it was forgotten. In the app, only the person sees that record for a personal memory, and every resident sees it for a shared one. The conversation in which the memory was first said is a separate record: it stays in the resident's history, where the assistant's search of past conversations can still find it, until they delete it, and

erasing their data removes both. A resident can also erase what the home has learned from them and what they have said to it while keeping their account: their personal memories, their conversations, the words of the spoken requests filed under their account, what they said at shared panels, the standing preferences they set and their signed-in questions to the website assistant. Their account and settings, their reminders and scheduled tasks, and what they added for the whole household stay. Elysium's website assistant is separate from the home: it keeps a signed-in person's questions and answers for 180 days to check the quality of answers and prevent abuse, and erasing their data or closing their account deletes them sooner. When the owner turns on the hub's nightly backups, each archive is by default deleted about 14 days after it was made, so an erased item leaves those copies on the same schedule. In the Sovereign placement there is no copy in a vendor datacenter to reconcile against.

We therefore treat two operations as requirements, listing what the home holds about a person and removing it on request, and the current version implements both.

7. Status and limitations

This section records the state of the system as of October 2026.

Operational today: the household model of distinct people with roles; household standing preferences (one active value for each room, setting and occasion, recording who set it), remembered and enforced across days, listed for every resident and removable; tiered access with device-type guest scoping and openly declined requests; review of extracted memories, each starting unreviewed until the resident confirms or forgets it; erasure on forgetting and on request, as described in Section 6; and storage of memory and preferences on the hub. These are exercised through the assistant's text interface and the household's dashboard.

In active integration: speech on the hub, with the wake decision made on the device. Before voice ships, the hub must either recognize who is speaking or treat an unrecognized voice like the shared wall panel, with household memory only and the guest set of actions. Until then voice remains in integration, and the home tells people apart by the credential they act through. Meanwhile the hub files every spoken request under one resident's account, chosen when the hub is set up, so in the app only that resident can read and erase the words.

When two residents state different values for the same room, setting and occasion, the most recent instruction wins and both are told: the resident whose setting was replaced receives a notice, and the person who replaced it learns whose setting they changed. A preference set by an administrator can be replaced or removed only by an administrator, and a child's instruction applies once and is never kept as a standing preference.

Some limits are intrinsic. Recognition of this kind is probabilistic and low-assurance by design: a shared or imitated voice proves nothing about identity [4, 5], so recognition is used to grant comfort and appropriate access and never stands in for a security credential where one is required. Locality protects the household against outside profiling. Trust among the people inside depends on the household itself, because the access model gives residents real reach across the home. Erasure reaches the hub's live records at once and its nightly backups as they age out. Backups the owner makes by hand, snapshots the hub keeps from before a restore and copies moved off the hub, an administrator's downloaded backup among them, keep what they held until whoever holds them deletes them, and in Hybrid the hub cannot recall what earlier

requests carried to the cloud model. And personalization improves with what the home remembers, which pulls against keeping little. Our response is review: each memory the assistant extracts is used from the moment it is made, is marked unreviewed, and can be confirmed or forgotten by the resident.

References

- [1] Nissenbaum, H. Privacy as Contextual Integrity. *Washington Law Review* 79(1):119, 2004.
- [2] Solove, D. J. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154(3):477-560, 2006. doi:10.2307/40041279
- [3] Bai, Z., and Zhang, X.-L. Speaker Recognition Based on Deep Learning: An Overview. *Neural Networks* 140:65-99, 2021. doi:10.1016/j.neunet.2021.03.004
- [4] Wu, Z., Evans, N., Kinnunen, T., Yamagishi, J., Alegre, F., and Li, H. Spoofing and Countermeasures for Speaker Verification: A Survey. *Speech Communication* 66:130-153, 2015. doi:10.1016/j.specom.2014.10.005
- [5] Wang, X., Yamagishi, J., Todisco, M., et al. ASVspoof 2019: A Large-Scale Public Database of Synthesized, Converted and Replayed Speech. *Computer Speech & Language* 64:101114, 2020. doi:10.1016/j.csl.2020.101114
- [6] Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., and Feamster, N. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2(2), 2018. doi:10.1145/3214262
- [7] Lau, J., Zimmerman, B., and Schaub, F. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2(CSCW), 2018. doi:10.1145/3274371
- [8] Meyer, P. *Sovereign by Construction*. Elysium Labs technical report ELY-TR-2026-01, 2026. elysium-labs.ai/research/sovereign-by-construction (<https://elysium-labs.ai/research/sovereign-by-construction>)
- [9] Meyer, P. *The Home That Grades Itself*. Elysium Labs technical report ELY-TR-2026-02, 2026. elysium-labs.ai/research/the-home-that-grades-itself (<https://elysium-labs.ai/research/the-home-that-grades-itself>)
- [10] Connectivity Standards Alliance. *Matter Core Specification*, Version 1.4. 2024. <https://csa-iot.org/all-solutions/matter/>
- [11] Amazon. Alexa and Alexa Device FAQs: voice recordings and voice ID. Accessed 10 October 2026. <https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230>

[12] Apple. Apple Platform Security: HomeKit camera security. Accessed 10 October 2026.
<https://support.apple.com/guide/security/sec525461d19/web>

How to cite

Meyer, P. (2026). Recognition Without Surveillance. Technical report ELY-TR-2026-03, version 1.3. Elysium Labs, Zürich, Switzerland. <https://elysium-labs.ai/research/recognition-without-surveillance>

Revision history

Version 1.3 · 11 October 2026

Corrected who can read a person's data. Version 1.2 said that only the person can read their personal memories, but an administrator can download a backup of the household that holds the words of every resident's personal memories without saying whose they are, and the hub's own backups copy its whole database, conversations included. Table 2 now says who can read each item in the app, a new paragraph after it describes both kinds of backup, and Section 7 counts an administrator's downloaded backup among the copies that keep erased items until they are deleted.

Version 1.2 · 10 October 2026

Rewrote the access model, the standing-preference rules, the data inventory and erasure to match what the product enforces in each placement. This corrects version 1.1, which limited a child to their own rooms and devices and a guest to the lights in shared rooms, and described only the Sovereign case, in which nothing about a resident leaves the house; in Hybrid a request carries its context to a cloud model, and an owner can also send spoken requests there. The arbitration between residents' standing preferences, which version 1.1 listed as planned, is now enforced and described, and both figures were redrawn to match the text. Added in-text citations and complete references; the page also gained a report number, citation formats, a PDF, table captions and references linked to their records and to the companion reports.

Version 1.1 · 26 July 2026

Named the author and labeled the report as self-published and not peer reviewed.

Version 1.0 · 12 July 2026

First published.