Privacy and Owner Control in the Robotic Home

Bystander protection and credible erasure

Allan Watkins
Laws of Robots series
Version 1.2 — 1 November 2026

Abstract

A robot moving through a home can encounter intimate information about people who never chose to use it. Its owner may have invited the machine; a visitor, a child, or a neighbor did not necessarily agree to become part of its record. This paper argues for bystander exclusion, owner control, and an erasure capability established before non-owner information is admitted. It examines documented failures involving household sensing and the four commitments in the published Privacy Commitments Statement, version 1.2. It reconciles those commitments with a dated synthetic development demonstration and the documented behavior of the key-storage platform. A configured retention period, permanent purge, recovery authority and the absence of other usable copies are separate matters. The operational account therefore identifies when erasure can be considered complete and which evidence supports that conclusion. Previously exported information and disposal of the owner's external identity link remain outside the mechanism. Owner authority and the owner's own information require protection throughout use, repair, transfer and retirement. Published rules and cryptographic checks support that work within their stated scopes; enforcement and coverage require evidence of their own. The case is for privacy requirements established before collection and accountable throughout the life of the robot.[1]

§1 — The inventory of one afternoon

The machine below is no particular product. It is an illustrative composite: a mobile robot with cameras, microphones, depth sensors, and some autonomy to move through a home and direct its attention. Imagine the following possible observations during an ordinary afternoon. The list is not a report of a test, or a claim that a particular product can resolve and retain every item.

1. The owner's face, forty-one times, from different angles and in different light.
2. The face of a woman who came to the door at 1:20 and stayed an hour. She has no account with the maker.
3. Her voice, and a conversation about a job she may leave and a diagnosis her mother received.
4. Prescription bottles on the kitchen counter, with their labels visible.
5. Mail on the hall table: a bank statement, a letter from a law office, a past-due notice.
6. Titles on the bookshelf.

7. A visiting child who gives the machine her name when it asks who is home.

8. The room layout and the location of a safe.

9. An argument at 3:40, including who was present and who apologized.

10. What the owner watched, and when he fell asleep.

11. A neighbor visible through the west window in her own yard.

12. Signs of which medicines were taken and which were skipped.

13. A passcode spoken aloud to a phone nearby.

14. The identity of a caller announced by a phone.

15. The dog's seizure, and the owner crying afterward at 4:15.

16. An uneventful hour that could reveal as much about a household's routine as an exceptional moment.

Sensing an event, inferring its meaning, retaining it, and sending it elsewhere are different acts. A design may allow one and prohibit another. Those distinctions determine what would actually enter a record. They also explain why a list of sensors is an inadequate privacy answer.

Stop at any line and ask who agreed to the relevant processing. The owner's purchase does not answer for everyone else. Even for the owner, agreeing to a useful function is not the same as understanding every destination, recipient, inference, and retention period attached to it. The question is what may become part of the machine's memory, who controls that decision, and what a person can later have erased.

§2 — Mobility, attention and the household

Mobility changes where observation can occur. A moving sensor may enter rooms beyond the position where it was first placed, or remain near a person. It still has physical limits, and exclusion zones, closed doors, operating modes, and controls can matter. The privacy question is whether those boundaries exist, how reliably they work, and what people nearby can understand about them.

Persistence changes the exposure. A machine that is available throughout the day may encounter recurring habits and relationships. Availability does not necessarily mean continuous recording. A useful privacy account must explain when sensing begins, when information is retained, and what switches or indicators actually control those acts.

Breadth of sensing can connect information that would otherwise remain separate. Images, voices, locations, and times may together identify a person or disclose a relationship. Autonomous attention adds a further question: what can the machine decide to inspect without an immediate human instruction, and what evidence shows that its attention remains within the intended limits?

These capabilities have precedents. Amazon's Astro documentation describes autonomous movement, cameras and microphones, on-device processing for some functions, cloud

processing for others, a sensor-off button, and out-of-bounds zones.[2] Those are manufacturer descriptions rather than an independent privacy assessment. They nevertheless show why the argument must examine actual data paths and controls rather than claim that every earlier device was stationary, passive, or incapable of protecting a room.

The concern is the combination of intimate access and delegated attention. A household member can invite the device while visitors and other residents bear some of its consequences. Privacy therefore belongs in the arrangement that governs the machine, from first operation through repair, changes of service or ownership, and retirement. It should not depend on every affected person discovering an obscure setting after the information has already been retained.

§3 — What the documented failures establish

Three records show why household data deserves that scrutiny. Their sources and circumstances differ, and the differences limit what can be inferred from them.

Eileen Guo's December 2022 investigation for MIT Technology Review examined screenshots shared in closed social-media groups by data workers. The images came from development versions of iRobot's Roomba robots, not ordinary retail devices. iRobot said the collectors had agreements to send training data and that the sharing violated its service-provider agreement. The report could not inspect those consent agreements. This is evidence of exposure in a development-data supply chain, including intimate household images; it does not establish that retail Roombas routinely upload the same material by default.[3]

In July 2023, the U.S. Department of Justice reported a court-entered settlement concerning Alexa. The government's complaint alleged excessive retention of children's recordings and failures to delete all information as represented. The stipulated order imposed a $25 million civil penalty and retention, deletion, and disclosure requirements. The allegations and agreed remedies should not be presented as findings from a contested trial.[4]

Apple's August 2019 statement acknowledged concerns about human review of Siri recordings and announced changes: audio retention would be off by default, participation in audio-based improvement would require opt-in, and review for participants would be limited to Apple employees. Computer-generated transcripts would continue to be used.[5] That dated statement supports both the concern about human access and the need to describe subsequent policy changes fairly.

The common question is what happens after information has entered a chain of custody. Who can see it, who receives copies, what a deletion request reaches, and what evidence supports the answer? These cases justify asking those questions. They do not prove one uniform industry architecture, that every deletion control merely hides data, or that every maker ignores bystanders.

The revised pattern paper argues for scrutiny independent of the interested party, access to evidence, and the ability to require correction.[6] Applied here, the lesson is to examine privacy assurances beyond the maker's account of its own good intentions. A privacy promise can contain useful information while still requiring evidence of enforcement.

§4 — Who is in the room

Return to the visitor. She came to see a friend, not to open an account with a device maker. If information about her is retained, the absence of an account should not be mistaken for the absence of an interest or an applicable right. A process designed only for the purchasing account holder may be a poor practical route for her even where the law provides protection.

The legal framework is not empty. The GDPR contains a personal-or-household exemption, while recital 18 distinguishes providers that supply the means of processing. Its rules also address identifiable information, lawful processing, erasure and privacy by design. Consent is one lawful basis, rather than the only possible basis. Erasure rights have conditions and exceptions, including specified legal obligations and legal claims. [7]

The boundaries depend on facts. In Ryneš, the Court of Justice held that home surveillance also covering public space fell outside the household exemption under the predecessor directive. [8] EDPB guidance considers circumstances inside private premises, including personal relationships, scale, frequency and effects on people; it also addresses access, erasure, disclosure and technical safeguards. [9] That is a useful foundation for assessing new devices, rather than a complete answer about every home robot.

The author's design position is that protections for people merely present should not rely solely on their ability to discover and enforce a claim after collection. Admission should be a deliberate decision for which someone is accountable. Owner authority over the machine must also be exercised consistently with other people's applicable rights. The privacy problem is practical as well as legal: the machine needs rules before the next visitor arrives.

§5 — Four published commitments

The following commitments come from the Privacy Commitments Statement, version 1.2, ratified July 23, 2026. The public page displayed that edition when checked on November 1. Its source file matches the checksum displayed beside it. Appendix A reproduces the statement unchanged, including its scope limits and authorship disclosure. [1]

COMMITTED means a published design and operating rule. It does not mean that this paper has independently verified every implementation path. **RECORDED DEMONSTRATION** identifies a dated test and its exposure tier. **DESIGN REQUIREMENT** identifies what a privacy assurance must establish beyond those results. Public availability of the rule is checkable; compliance with it is a separate question.

5.1 Bystanders are excluded by default

The statement says: *"The machine's perception of anyone other than the owner does not enter the record."* It then specifies the exception: information about a non-owner may enter only through an explicit, deliberate, attributed act of admission tied to a reason for accountability. Speaking to the machine or answering its questions does not itself create that route. [1]

That is a committed rule about the decision record. A complete privacy account must also explain what happens before an entry is sealed and outside that record: transient processing,

diagnostic material, external services, and derived information. Excluding a bystander from one record is not proof that no information about that person exists anywhere else.

Nor does replacing a name with a token necessarily make information anonymous. Relationships, locations and other context may still permit identification. [7] A review that finds no names supports its stated search result; it cannot alone establish the absence of all personal information across a system. The evidence must match the scope of the claim.

5.2 Erasure is established before non-owner data is admitted

The statement's collection restriction is specific: the system will not collect personal data about anyone other than the owner until the capability to erase it completely and provably is operational. Its v1.2 account reports a development demonstration involving fifty synthetic subjects, with key destruction verified on July 21, 2026. It also states that the collection restriction remains in place: the first entries of the live admission path must be exercised with synthetic subjects before real third-party data is admitted. [1]

The July 21 operator record reports authorized reads returning empty live-key and deleted-key lists for the development vault, together with the configured retention and purge-protection properties. It documents completion of the previously pending check for that demonstration. It does not claim a production-tier erasure test or an independent external audit. [10]

The ordering remains the argument's center: establish the promised erasure path before admitting the information it is supposed to erase. The paper retains that requirement. The demonstration supports the development result at its recorded scope; it does not establish every surface, later deployment or real request. The published restriction addresses non-owner data. The owner's information remains subject to the lifetime protections argued for in §7, whose implementation is not established by this synthetic demonstration.

5.3 Content is erased while sealed structure remains verifiable

The statement commits to destroying the key that makes protected entry content readable while retaining the sealed sequence. Its v1.2 wording describes a capped destruction window, currently seven days, no standing reversal permission, no key backups and no standing backup capability. [1] This paper preserves the commitment to completed erasure while distinguishing the platform's rules, the dated configuration and the conditions required for that result.

Retention and completion. Microsoft documents that the retention interval is fixed when the vault is created. With purge protection enabled, an object cannot be purged early; an appropriately authorized principal can still recover it during retention. Unless recovered, the object is scheduled for permanent purge after retention expires. [11] The seven-day setting in the July record is therefore a retention configuration. It is not, by itself, evidence of a maximum elapsed completion time for every erasure. Here, completed key destruction means a verified permanent-purge result, rather than the arrival of a calendar date. The July 21 authorized empty live and deleted listings establish that result for the tested development vault, read together with the prior demonstration record. [10]

Standing permissions and administrative power. The July 21 role inventory records no standing recovery or key-backup permission on that vault. It also records that a subscription

administrator could grant additional permissions later.[10] Microsoft documents the roles that can manage those assignments.[17] The evidence supports a dated absence of standing permission, not technical impossibility of acquiring it. A later recovery or usable backup would defeat a claim that destruction had completed under the promised conditions; the absence of such powers must remain an operating requirement rather than be inferred forever from the July snapshot.

Other usable copies. Microsoft documents that a restored key copy is independent of its source: purging the original does not invalidate a previously created backup or restored copy.[16] The July inventory does not prove that no backup existed earlier. NIST's cryptographic-erasure guidance also requires attention to every relevant key copy and to plaintext outside the encryption boundary.[12] Permanent unreadability of protected content consequently depends on effective encryption, destruction of all usable key copies and the absence of readable copies within the claimed scope. A failed decryption attempt or an empty vault listing alone cannot establish all those conditions.

This is the operational meaning used throughout the paper. The published v1.2 sentence about a capped window remains a historical statement of commitment in Appendix A; it is not repeated here as an independently established platform guarantee. The commitment's standard remains complete erasure before non-owner information is admitted. Where its conditions have not been demonstrated, the paper states a requirement to meet, rather than a result already achieved.

The privacy benefit remains compatible with structural accountability. Verification may establish that a sealed entry occupies a particular place in an intact sequence without revealing its contents. Once those contents are erased, their meaning may no longer be reconstructable. Preserving the envelope is not the same as preserving a readable account of everything the machine did.

5.4 Storage surfaces are covered and limits are disclosed

The statement commits the erasure guarantee to every surface where the person's data can reside, without permanent exceptions. It also requires construction gaps to be named internally with a completion deadline.[1] The public document establishes that rule; it does not expose the full inventory or independently establish compliance with it.

The rule must be read with the statement's explicit limits. The mechanism does not reach information already exported or disclosed from the record. When third-party data is admitted, the owner alone is to hold the link between a person and the relevant entries, outside the system. Disposing of that link is the owner's act, which the system does not perform or verify.[1] These are material boundaries, not details to omit from a headline erasure claim.

A credible account identifies which copies and surfaces are under the system's control, what happens to them, and what remains outside its reach. Calling a backup or an analytics copy a different surface cannot by itself explain why a person should believe it was erased. Conversely, an erasure mechanism should not promise control over a copy already placed beyond its custody.

§6 — Refusal and the evidence for it

A published refusal can make an assurance more precise. It tells a relying party what the system declines to admit, under what conditions that could change, and where to look for the versioned rule. Retained versions and a published checksum help a reader identify the statement being relied upon. They make comparisons possible.[1]

That is a documentary property. A rule against collection is not, by itself, evidence that no collection occurred. An implementation can depart from its documentation without revising the public page. A visible admission route is valuable only to the extent that the assurance case establishes its coverage and the absence of relevant bypasses. Publishing a rule does not force a violation to record itself.

Independent retention, protected recording paths and checks of actual data flows can strengthen the evidence, under their stated assumptions. The revised breach paper treats these as properties to demonstrate and requirements to test, rather than universal guarantees that every compromise becomes visible.[13] The same discipline applies to privacy. A record should help expose a departure from a rule, but a valid signature does not establish that no unrecorded departure occurred.

The stronger case for refusal is therefore specific. It reduces the information the design permits itself to hold and gives outsiders a clear standard against which to examine behavior. Evidence of enforcement must then be supplied at the relevant boundary. The aim is to make an assurance challengeable, rather than to substitute a public promise for the independent scrutiny the series argues for.

§7 — Owner control and responsibility

The owner should direct the machine and answer for the authority delegated to it. A robot acting as an extension of its owner's judgment should not turn access to the household into an entitlement for its maker to retain the household's information. That is the author's governance position. It concerns control and responsibility, rather than a claim that device ownership extinguishes anyone else's privacy rights.

The same position covers the owner's information throughout the robot's life. The owner should be able to understand and control what is retained, who can read it, what repair or support access permits, and what happens when an account, service or ownership arrangement ends. Resale or retirement of the device does not by itself settle the fate of copies held elsewhere. Those are requirements of the model advanced here, not capabilities established by the non-owner erasure demonstration. An adequate implementation account must address them directly.

Admission should therefore have an accountable actor, and a person seeking erasure needs a practicable route to whoever is responsible for the relevant processing. Operational control of an erasure function and a data subject's applicable right to request erasure are different matters. An owner's involvement cannot be offered as a reason that another person's rights disappear. Applicable law can also require preservation in particular circumstances; this paper does not declare those obligations inapplicable.[7,9]

Checking a record and reading its protected contents are also different acts. The public verification specification distinguishes a public, certifier-signed checkpoint from an authorized full-record chain inspection over encrypted envelopes.[14] The companion paper's October 31 rehearsal authenticated the public checkpoint from saved inputs and reproduced the shared bounded values; it did not independently walk the private chain.[15]

A stamp therefore does not prove that every action was captured, that no personal information escaped elsewhere, or that the erasure commitments are satisfied. Erased content can leave useful structural evidence without leaving a readable reconstruction. Owner control, confidentiality and evidential integrity are requirements that must be evaluated together, with the limits of each stated.

The certifying role remains report-only. It does not acquire authority to command, seize or disable the machine because it reports a status. Architectural separation of functions also does not establish institutional independence, independent key custody or an external privacy audit. The revised companion papers distinguish those questions; this paper does not upgrade their evidence into certification of privacy compliance.[13,15]

§8 — What the present evidence establishes

The published statement is v1.2, dated July 23, 2026, as observed on November 1. It reports the synthetic development demonstration and states that the non-owner collection restriction remains in place. The July 21 operator record establishes the tested development vault's empty live and deleted listings and dated permission inventory. Section 5 identifies exactly which conclusions follow from those observations.[1,10]

This is evidence for a bounded demonstration, not an independent audit of the whole service. The paper makes no new claim about current global collection, every storage surface, real-person erasure or a changed deployment. A search for names cannot establish the absence of all personal information. The published statement itself discloses that outsiders cannot inspect the empty state and that no third party audits these commitments. Its export and external-identity-link limits remain part of the account.[1]

The argument rests on explicit requirements and evidence within those boundaries. As in the revised pattern paper, independent examination and the ability to require correction remain necessary parts of a trustworthy arrangement.[6]

§9 — Ten questions before it crosses the threshold

These questions apply to a machine from any maker. A useful answer identifies the scope, the responsible party and the evidence, rather than relying on a reassuring label.

1. **Does information about my visitors enter the record by default?** Ask what is perceived, retained and transmitted, which bystanders are excluded, and whether an exception requires deliberate admission.
2. **What records an admission and what can bypass that path?** Ask who authorized it, why it was needed, and what testing establishes the path's coverage.

3. **When I delete something, what actually happens?** Ask which information becomes unavailable immediately, when destruction completes, and whether recovery remains possible in between.

4. **Which copies does erasure reach?** Ask separately about the record, backups, diagnostic logs, external processing, derived data and prior exports.

5. **What can remain, and why?** Ask about residual metadata, applicable retention obligations, and any limits on identification or erasure. A stated exception can be examined; an undisclosed one cannot.

6. **What survives erasure as evidence?** Ask what remains verifiable about an entry and what can no longer be reconstructed once the protected contents are gone.

7. **Who controls the keys and the recovery powers?** Ask about owner, service operator and platform roles, including backups and privileged access. The word "cloud" does not answer those questions either way.

8. **Who can read or disclose the information?** Ask about actual processing access, retained copies, metadata, exports and legal demands. A restriction on one encrypted record does not describe every copy.

9. **Where are the promises and their history?** Ask for the published version, its scope and retained predecessors, alongside evidence that the implementation follows it.

10. **What happens over the whole life of the machine?** Ask about loss, repair, account changes, service closure, resale, return and retirement, including information held away from the device.

The case for these questions does not depend on a claim that every product fails them. It depends on the intimacy of what a home robot may encounter and the difficulty of recovering privacy once information has escaped. The owner deserves meaningful control of the machine's memory. People merely present deserve protection that does not depend on becoming customers first. Both deserve an erasure answer whose scope can be understood before collection begins.

Privacy and owner control in the robotic home begin with decisions made before information is retained. Keep bystanders out of the decision record by default. Establish the specified erasure path before admitting non-owner information, and report completion only at the scope the evidence supports. Preserve verifiable structure while acknowledging the loss of erased meaning. Protect the owner's information through use, repair, transfer and retirement. These requirements preserve the value of a machine acting on its owner's authority while making its treatment of everyone nearby open to examination and correction.

Appendix A — Privacy Commitments Statement v1.2

Published v1.2, ratified July 23, 2026, is reproduced verbatim. Its source matches the checksum displayed on the public page when checked November 1, 2026. [1]

Evidence and scope. Section 5.3 reconciles the statement's stronger technical wording with the demonstrated result: seven days is the retention setting; completion requires verified purge and the stated copy boundaries. The July permission snapshot does not prevent later administrative grants. These published commitments remain requirements; this reproduction does not certify their unconditional technical enforcement. [10–12,16,17]

Privacy Commitments Statement

Version: 1.2

Status: Public-facing statement of record; versioned; digest-pinnable

Identity: Laws Of Robots (product-side governance artifact)

Authorship: Owner-ratified; wording drafted with AI assistance; the owner owns every commitment

Date: 2026-07-23

Relationship: Companion to the internal erasure-posture doctrine. Cited by the privacy whitepaper. Consistent with both by construction.

§1 — Purpose and scope

This document is the binding public statement of the system's privacy commitments. It is not a privacy policy, not legal terms, and not a feature description.

"Binding" here means published, versioned, and changed only in the open. The commitments below govern the system's design and operation. Any revision is itself a visible, dated act.

§2 — The four commitments

2.1 Bystander exclusion

The machine's perception of anyone other than the owner does not enter the record. This includes visitors, children, neighbors visible through windows — anyone merely present in its environment. Interacting with the machine, speaking to it, or answering its questions does not create a route into the record. Admission, defined below, is the only route.

Information about a person other than the owner may enter the record only through an explicit act of admission. That act must be deliberate, attributed to the person performing it, and tied to a clear reason for accountability. There is no passive or automatic route by which a bystander's information becomes part of the machine's record.

2.2 The hard gate

The system will not collect personal data about any person other than the owner until the capability to erase that data completely and provably is operational.

That capability has now been built and demonstrated: in a development environment, fifty synthetic test subjects were erased by key destruction, and the destruction of their keys was verified on 2026-07-21. The gate remains closed. It opens only when erasure has been proven on the first entries of the live path that would carry a third party's data — exercised with synthetic subjects before any real person's data is ever admitted. Until then, the record contains no personal data about any third party. The gate does not merely slow collection — it forbids it.

2.3 Erasure semantics

Erasure is performed by destroying the key that makes an entry's content readable. Key destruction completes within a bounded, capped window that no one — including the owner — can shorten, extend, or override; that window is currently seven days. No standing permission to reverse a destruction during that window exists, no backup of an erasure key is ever taken, and no standing capability to take one exists. Once destruction completes, the content is permanently unrecoverable. The sealed entry remains in the record — its position in the sequence, its integrity, and the fact that a decision occurred stay intact and verifiable.

This approach makes privacy and accountability complements rather than opposites. A person's information can be destroyed on request, but the tamper-evident record of what the machine did cannot be altered or erased by anyone, including the owner.

2.4 No permanent carve-outs

The erasure guarantee applies to every surface where a person's data can reside. There are no permanent exceptions.

Where a gap exists during construction, that gap must be explicitly named and given a completion deadline internally. An unnamed or unclocked gap is treated as a violation of the commitment, not an oversight.

§3 — What these commitments do not claim

Stated plainly, in one place:

- The erasure mechanism has been demonstrated on synthetic subjects in a development environment. It has not yet been exercised on any real person's data — the record holds none.
- Erasure destroys the sealed entry's content. It does not reach information exported or disclosed from the record before the erasure occurred.
- When third-party data is admitted, the link between a person and their entries will be held by the owner alone, outside the system. Disposing of that link on erasure is the owner's own act; the system does not perform or verify it.
- Key destruction is carried out by the managed key-storage platform that holds the keys; the system relies on the platform to enforce the destruction window. That enforcement was verified in practice on 2026-07-21.
- The empty state cannot be inspected from outside.
- No third party audits or certifies these commitments today.
- The commitments bind this system's design and operation, not the law of any jurisdiction.

§4 — Change discipline

These commitments may be strengthened or added to. They may not be weakened or removed. Every version is retained and publicly comparable to the last.

§5 — Definitions

- **Bystander** — Any person the machine perceives who is not the owner.
- **The record** — The sealed, tamper-evident sequence of the machine's decisions.
- **Key destruction** — Erasure performed by destroying the key that makes an entry's content readable, leaving the sealed entry in place.
- **Destruction window** — The bounded, capped period between the start of key destruction and its completion.
- **Admission** — The deliberate, attributed act by which information about a person other than the owner is entered into the record.

The definitions in this Statement are authoritative. The privacy whitepaper's corresponding definitions conform to them.

Verification hooks

- **Version number:** 1.2 (this document)
- **Ratified:** 2026-07-23
- **Publication date:** 2026-07-23
- **Stable URL:** https://lawsofrobots.com/privacy-commitments/ — every version retained at a permanent path beneath it
- **Digest:** published beside this document at the stable URL, computed at build time over the exact bytes of this document's source file

Version history

- v1.0 — 2026-07-07 — initial text (superseded before URL assignment; never published)
- v1.1 — 2026-07-07 — §2.1 first paragraph tightened to admission-only; §3 meta-commentary sentence removed
- v1.2 — 2026-07-23 — §2.2 and §3 updated from "not yet built" to the demonstrated state of the erasure mechanism, with the gate's discharge standard stated publicly; §2.3 restated as the precise destruction sequence (bounded, capped window; standing-reversal and backup refusals added; end-state unchanged — permanently unrecoverable once destruction completes); scope limits added to §3; destruction-window definition added; stable URL assigned; authorship line corrected to disclosed provenance; identity line aligned to brand casing. First published version.

End of Privacy Commitments Statement v1.2

Appendix B — The four commitments at a glance

Commitment	Published scope	Evidence described	Limit that travels with it
Bystander exclusion	Non-owner information enters the decision record only through deliberate, attributed admission.	Published rule and version history. [1]	A record rule alone does not establish every sensor, processing or storage path.
Erasure before collection	The non-owner collection restriction remains until the specified synthetic proof on the live admission path.	Synthetic development demonstration; July 21 operator purge-verification record. [1,10]	No real-person or production-tier erasure test is established here; owner data needs its own account.
Content erased and structure retained	Complete key destruction is required; the sealed sequence remains.	July 21 purge state and standing-role inventory; platform retention and backup rules. [10–12,16,17]	Retention is not completion. Recovery, prior backups, other usable copies and loss of erased meaning remain distinct.
No permanent carve-outs	System storage surfaces are included; construction gaps must be named internally.	Published rule and explicit scope disclosures. [1]	Prior exports are outside the mechanism; disposal of the external identity link is the owner's unverified act.

References

[1] Laws Of Robots, *Privacy Commitments Statement*, v1.2, ratified July 23, 2026; §§2–4, verification hooks and version history. Public page and source checksum checked November 1, 2026. Current page; permanent version; source file.

[2] Amazon, *Amazon Astro Privacy*, questions 4–11, especially sensor power controls, on-device navigation, mapping and out-of-bounds zones. Manufacturer description checked November 1, 2026; not an independent test or claim of present sales availability. Product documentation.

[3] Eileen Guo, *A Roomba Recorded a Woman on the Toilet. How Did Screenshots End Up on Facebook?*, MIT Technology Review (December 19, 2022), opening incident account, iRobot response, and How and why our data ends up halfway around the world. Original report read in the browser November 1, 2026. Original investigation.

[4] U.S. Department of Justice, *Amazon Agrees to Injunctive Relief and $25 Million Civil Penalty for Alleged Violations of Children's Privacy Law Relating to Alexa* (July 19, 2023), complaint allegations and description of the stipulated order entered that day. Official account.

[5] Apple, *Improving Siri's Privacy Protections* (August 28, 2019), prior grading process and Changes We're Making. A dated account of announced changes, not a present implementation audit. Original company statement.

[6] Allan Watkins, *The Maker Has Always Graded Its Own Homework*, v1.2 (October 31, 2026), Abstract and concluding institutional argument. Companion paper in this series.

[7] Regulation (EU) 2016/679, recitals 18 and 26; Articles 2(2)(c), 4(1)–(2), 6, 12, 17 and 25. Original text inspected on EUR-Lex November 1, 2026. Official text.

[8] Court of Justice of the European Union, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428 (December 11, 2014), paras. 30–35. Judgment under Directive 95/46/EC; no claim that it decides all robot deployments. Original judgment.

[9] European Data Protection Board, *Guidelines 3/2019 on Processing of Personal Data Through Video Devices*, adopted January 29, 2020, with February 26 correction; §§2.3, 3, 6, 8–9, especially para. 13 and the access/erasure discussion. Official guidance.

[10] *Phase 40 Close — Purge-Verification Ceremony Record* (July 21, 2026), operator record, §§1–3 and 5–6, especially F-PV-01. Records the development vault's authorized empty live/deleted listings, standing-role inventory and limits concerning earlier backups and later administrative grants. Unpublished working evidence, model-drafted from owner-supplied outputs; not an external audit. The public statement [1] reports the corresponding demonstration.

[11] Microsoft, *Azure Key Vault: Soft-Delete Overview*, Soft-delete behavior, Purge protection and Key vault object recovery, checked November 1, 2026. Vendor documentation.

[12] Ramaswamy Chandramouli and Eric A. Hibbard, *Guidelines for Media Sanitization*, NIST SP 800-88 Rev. 2 (September 2025), §§3.2.1–3.2.5, printed pp. 12–16. Original guidance.

[13] Allan Watkins, *The First Machine Whose Breach Moves*, v1.1 (October 31, 2026), §§6–8 and Appendix B. Companion paper in this series.

[14] *Independent Verification Specification*, v1, §§0, 2.1 and 5, checked November 1, 2026. Public checkpoint authentication and authorized chain verification are separate exposure tiers. Published specification.

[15] Allan Watkins, *An Anchor Outside the Industry*, v1.1 (October 31, 2026), §§4.1–4.5 and revised Appendix A, including the October 31 local reference-verifier rehearsal. Companion paper in this series.

[16] Microsoft, *Azure Key Vault Backup and Restore*, Design considerations and Security considerations, checked November 1, 2026. Previously backed-up or restored keys are independent of subsequent source-key deletion. Vendor documentation.

[17] Microsoft, *Grant Permission to Applications to Access an Azure Key Vault Using Azure RBAC*, Managing built-in Key Vault data plane role assignments and Prerequisites, checked November 1, 2026. Administrative assignment authority is separate from a standing key data-plane grant. Vendor documentation.

Colophon

Allan Watkins

Laws of Robots series

Version 1.2 — 1 November 2026

This document is part of the Laws of Robots governance whitepaper series. The commitments reproduced in Appendix A retain their published authorship and change discipline.