

AUTHORITY DOES NOT TRAVEL BY DEFAULT

Legal Provenance and Revalidation in Persistent Human–AI Continuity

Operant Dyad — Paper 3
Micheal Preble
Independent Researcher
ORCID: 0009-0005-3906-6028
August 26, 2026

ABSTRACT

Persistent human–AI interaction can produce accumulated relationship state that remains useful across sessions, applications, models, and providers. The persistence of that state, however, does not establish that the authority governing its use persists unchanged. Different components of a continuity package may be governed by consent, contract, statute, institutional role, fiduciary duty, delegation, court order, guardianship, succession, confidentiality, mandatory retention, or other external sources of authority. Those sources can differ in scope, purpose, object, recipient, jurisdiction, and duration, and they can change while the underlying state remains historically intact. This paper examines the legal and institutional configuration problem created when persistent human–AI relationship state crosses technical or organizational boundaries. It argues that ownership is too coarse a master variable, that technical portability is not equivalent to lawful portability, and that source-side authority should not be treated as a context-free status that automatically survives migration. Existing law and standards already provide much of the necessary machinery, including contextual authorization, policy decision and enforcement, credential provenance, revocation, selective disclosure, delegation, provider switching, fiduciary access, retention, and remedies. The residual problem is therefore narrow: continuity architectures should preserve legally material provenance and authority-state information sufficiently for a receiving system to re-evaluate current legal operability before using, disclosing, inferring from, or acting upon transferred state. The paper treats this as a synthesis and configuration requirement rather than a new legal right, ownership regime, or authorization primitive.

KEYWORDS

human–AI interaction; relationship state; AI continuity; legal authority; provenance; portability; provider switching; delegation; digital succession; authorization; AI governance; Operant Dyad

1. INTRODUCTION: THE AUTHORITY PROBLEM

Persistent interaction changes the practical character of an AI system. A model that encounters a person once may need little more than the immediate prompt. A system used repeatedly can accumulate corrections, decisions, constraints, preferences, working history, interpretations, and other state that changes later interaction. Earlier papers in the Operant Dyad series describe that accumulated material as Relationship State and examine the technical and governance mechanisms by which selected state might persist without making one provider, model, or application the permanent custodian of the relationship. Paper 3 begins where that architectural question becomes a question of authority. A state

item can remain technically available after the legal basis for using it has narrowed, expired, moved to another actor, or become dependent on a different context.

This distinction matters because continuity encourages movement. A person may change providers, use several models, authorize an agent, enter an employment or institutional context, lose decision-making capacity, appoint a fiduciary, or die. The underlying record may survive each transition. The legal significance of the record does not necessarily survive in the same form. A fact learned in one setting may remain true while disclosure becomes prohibited. A delegated permission may remain documented after the delegation has ended. A record may be subject to preservation or retention requirements without that requirement itself authorizing unrelated operational use, disclosure, inference, personalization, or transfer. A provider may be technically capable of transferring state that the destination is not entitled to use for the same purpose.¹

The resulting problem is easy to obscure if authority is represented as a property of the data itself. The relevant question is not simply whether an item is 'authorized.' It is authorized by whom, under what source, for which operation, concerning which object, for what purpose, to which recipient, in which institutional and jurisdictional setting, and during what period. Those dimensions are familiar to mature access-control, identity, credential, privacy, records-management, fiduciary, and regulatory systems. Paper 3 does not claim to invent them. Its narrower claim is that persistent human–AI continuity can combine heterogeneous state governed by several of them at once, and that a continuity architecture should not erase those distinctions when state crosses a boundary.

The paper therefore advances a configuration requirement rather than a new legal doctrine. Legally material provenance and authority-state information should remain sufficiently attached to consequential continuity state that a receiving system can evaluate current operability in its own context. Technical validity, possession, authentication, and source-side permission are inputs to that evaluation; none should be treated as a portable substitute for it. This approach also places a boundary around the person-centered principle developed in the broader project. The natural person can remain the enduring architectural reference point across replaceable providers without being declared the universal owner or unilateral legal controller of every record associated with the relationship.

2. WHY OWNERSHIP IS AN INADEQUATE MASTER VARIABLE

Ownership is attractive because it appears to simplify the problem. If accumulated relationship state could simply be declared the property of the person, portability, deletion, access, inheritance, and control might seem to follow from one rule. Texas privacy law illustrates why that compression is unsafe. The Texas Data Privacy and Security Act creates distinct rights to access covered personal data, correct inaccuracies, request deletion, obtain a portable copy of certain consumer-provided data, and opt out of specified processing; it does not state that consumers own all personal data about them. Those rights operate under different predicates and alongside authentication requirements, controller

¹ See *infra* note 25 (collecting illustrative, domain-specific preservation, retention, and restriction authorities).

and processor duties, entity and data exemptions, permissible retention and processing grounds, and special treatment of pseudonymous and deidentified data.² A statutory right concerning data is therefore not necessarily a property right in the data.

Relationship State makes the weakness of an ownership-only approach more visible because the state itself is heterogeneous. Some items may be direct statements by the person. Others may be machine inferences, provider-generated metadata, institutional records, third-party statements, or derived representations assembled for a specific purpose. Texas's statutory categories do not justify forcing all of those technical objects into one rights bucket. Personal data turns first on whether information is linked or reasonably linkable to an identified or identifiable individual, followed by applicable role, entity, data-class, deidentification, pseudonymization, and other statutory rules. The Act recognizes automated profiling, but the statutory text audited does not expressly resolve whether every inference, generated profile, summary, embedding, probabilistic classification, or other derived representation is independently subject to correction or deletion. That silence is a textual observation, not a conclusion that those outputs necessarily fall outside Chapter 541. Paper 3 therefore preserves those AI-object classifications as unresolved rather than converting a privacy right into universal authority over derived state.³

For continuity design, the useful move is therefore to separate the incidents that ownership language tends to collapse. Access, correction, restriction, use, disclosure, portability, custody, retention, delegation, revocation, action authority, and remedies can be represented as different questions. The answer to one may inform another, but it does not mechanically determine it. This does not require rejecting property law or ownership concepts where they actually apply. It requires refusing to make ownership do analytical work that existing law assigns to several different doctrines and institutional relationships.

That separation also prevents the person-centered architecture from becoming a legal overclaim. The Permanent Primitive principle treats the person as the durable reference point while providers, models, applications, representations, and transport mechanisms remain replaceable. In Paper 3, that is a design posture, not a declaration that every associated datum legally belongs to the person. The architecture should preserve the person's continuity and legitimate agency while remaining capable of representing external duties, competing rights, institutional constraints, and changes in lawful authority.

3. MULTI-SOURCE, MULTI-INCIDENT AUTHORITY

Once ownership is removed as the single master variable, authority can be treated more precisely. A continuity operation may be legitimate because of consent, contract, statute, regulation, organizational role, agency, fiduciary duty, a power of attorney, guardianship, a court order, succession

² Tex. Bus. & Com. Code §§ 541.001(2), (19), (22), (24), (26), 541.002–.003, 541.051(b), 541.052(e)–(f), 541.101, 541.104, 541.106, 541.202, 541.204.

³ Tex. Bus. & Com. Code §§ 541.001(19), (22), (24), (26), 541.051(b)(2)–(3), 541.106.

authority, a retention obligation, confidentiality rules, or another recognized source. These sources are not interchangeable. They can authorize different actors, cover different objects, permit different operations, and expire or change under different conditions.⁴

Technical authorization systems already provide useful analogues. NIST's attribute-based access-control model evaluates attributes concerning the subject, object, requested operation, and sometimes the environment against applicable policy. XACML separates policy administration, policy information, policy decision, and policy enforcement, and its architecture can represent policy issuers and delegated administration. These are strong implementation neighbors because they demonstrate that authorization need not be a permanent property attached to an object. A decision can instead be produced from current attributes, policy, relationships, and context.⁵

The legal layer adds a problem those mechanisms cannot solve by themselves: the legitimacy and continued applicability of their inputs come from outside the policy engine. A system can faithfully evaluate a policy that no longer represents the actor's legal authority. A credential can be cryptographically valid while the claim it contains is insufficient for the recipient's intended use. An employee's role can be accurately represented while the employee remains prohibited from moving confidential material to a personal AI account. The architecture therefore needs both decision machinery and reliable information about the external authority on which the decision depends.

For Paper 3, this produces a multi-source, multi-incident model. The source identifies where authority originates. The incident identifies what the authority permits or requires: use, disclosure, correction, restriction, deletion, retention, migration, delegation, action, audit, or challenge. Additional dimensions can identify the relevant object, purpose, recipient, institution, jurisdiction, and temporal state. The model is not offered as a new legal taxonomy. It is a way of preventing a continuity system from compressing legally different permissions and duties into a single portable status.

4. AUTHORITY HAS LIFECYCLE STATE

The underlying continuity record and the authority governing it can move on different timelines. A statement can remain part of the historical record after consent for a particular use has been withdrawn. A delegation can expire while the actions taken during its valid period remain auditable. A court order can supersede an earlier arrangement. A credential can be revoked. An institutional duty can require a record to be retained after its ordinary operational use has ended.⁶

⁴ See, e.g., Tex. Est. Code §§ 751.031, 751.131–.134, 1101.101, 1101.152, 1106.005, 1151.351, 1357.002, 1357.052, 2001.003, 2001.051–.053, 2001.101–.102, 2001.201, 2001.231; Tex. Bus. & Com. Code §§ 541.051–.053, 541.101–.106, 541.151–.156.

⁵ NIST SP 800-162 § 2 (Jan. 2014; updates through Aug. 2, 2019); OASIS, eXtensible Access Control Markup Language (XACML) Version 3.0 § 1.1.1, OASIS Standard (Jan. 22, 2013); OASIS, XACML v3.0 Administration and Delegation Profile Version 1.0 §§ 2–4, Committee Specification Draft 04 / Public Review Draft 02 (Nov. 13, 2014).

⁶ See *infra* note 25.

This is why deletion cannot serve as the universal response to lost authority. Deletion may be required in some circumstances and prohibited or unavailable in others. A system may instead need to preserve a record while marking it non-operative for ordinary inference, disclosure, personalization, or action. That distinction is familiar in records management and regulated environments, where preservation and permissible operational use are separate questions. Paper 3 uses the term retained-but-non-operative state for this architectural condition; the term is descriptive and does not assert a new legal category.⁷

Mature credential and identity systems again provide useful implementation neighbors. The W3C Verifiable Credentials Data Model supports validity periods, status information such as suspension or revocation, evidence, terms of use, and verifier-side evaluation. Shared Signals and Continuous Access Evaluation mechanisms address the danger of relying on stale security assumptions by communicating events that can require access to be attenuated or reconsidered. These systems reinforce the basic point that a previously valid state should not be assumed to remain valid forever merely because it can still be presented.⁸

The legal analogy must remain bounded. Revoking an access token is not the same thing as terminating legal authority, and a credential-status service does not determine whether a fiduciary still has a statutory power. The relevance is architectural. Continuity systems need a way to preserve history without treating historical authorization as perpetual authorization, and mature systems already demonstrate several ways to separate the two.

5. PROVIDER MIGRATION: TECHNICAL PORTABILITY IS NOT LAWFUL PORTABILITY

Provider exit is one of the clearest tests of persistent continuity. A person who has spent months or years building a useful working relationship with an AI system may reasonably want to move when pricing, access, product strategy, model behavior, institutional policy, or personal preference changes. A technically mature continuity architecture should make that transition possible without requiring the person to reconstruct every useful correction, preference, constraint, and decision from zero. Paper 2 treats this as a problem of functional portability. Paper 3 adds a separate question: which parts of the portable package can lawfully move and remain usable at the destination?

The distinction prevents a common conceptual shortcut. A successful export proves that information can be transported. It does not prove that the exporter possessed every legal incident necessary for the destination's intended use. Texas privacy law supplies a concrete example of the difference between legal portability and functional continuity. Where covered data is digitally available, Chapter 541 provides portability for a copy of personal data previously provided by the

⁷ See *infra* note 25.

⁸ W3C, Verifiable Credentials Data Model v2.0 §§ 4.9–4.10, 5.5–5.6, 7.1 & app. A (Recommendation, May 15, 2025); OpenID Foundation, OpenID Shared Signals Framework Specification 1.0 (Final Specification, Aug. 29, 2025); OpenID Continuous Access Evaluation Profile 1.0 (Final Specification, Aug. 29, 2025).

consumer in a portable and, where technically feasible, readily usable format that allows transmission to another controller without hindrance. The audited text does not require recreation of service functionality, transfer of controller-generated inferences or behavioral models, preservation of continuity provenance or authority state, migration of embeddings or internal representations, or equivalent destination performance.⁹ Statutory portability is therefore a mature legal mechanism, but it is not by itself Paper 2's functional migration.

The European Union's Data Act supplies a strong mature neighbor for switching and functional portability in covered data-processing services. Its switching framework addresses contractual obstacles, data and digital-asset porting, interoperability information, source- and destination-side responsibilities, and functional equivalence in defined circumstances. The Act also limits what the switching package must contain: Article 25(2)(f) requires the switching contract to identify categories of internal-functioning data excluded from export where export would risk breaching the provider's trade secrets, and Article 30(6) does not require disclosure or transfer of digital assets protected by intellectual property rights or constituting a trade secret. That limitation links the switching analysis here to the trade-secret constraints discussed in Section 7. The regime therefore strengthens the distinction between switchability, continuity, and destination legal operability without supplying a universal authority-transfer rule.¹⁰

A useful provider-exit test therefore has two halves. The first asks whether enough state can move for the relationship to remain functionally useful. The second asks whether the destination has enough provenance and current authority information to determine what it may lawfully do with that state. A system that solves only the first half can create continuity by copying ambiguity.

6. DESTINATION-SIDE REVALIDATION

The paper's narrow residual appears at the destination. Mature systems already know how to evaluate policies, verify credentials, process revocation signals, restrict disclosure, and make contextual authorization decisions. The remaining continuity question is whether the information needed for those mechanisms survives the migration of heterogeneous relationship state.

Consider a state item accompanied by a technically valid assertion that it was authorized for use in the source environment. That assertion may be accurate and still be insufficient at the destination. The recipient may be a different legal entity. The purpose may have changed. The person's role may have changed. A delegation may have expired. The destination may operate under a different jurisdiction or institutional duty. The item may include third-party material that was permissible in the original context but not for the new use. The correct question is therefore not merely whether the source assertion verifies. It is whether the asserted authority remains operative for the destination's proposed operation.

⁹ Tex. Bus. & Com. Code § 541.051(b)(4).

¹⁰ Regulation (EU) 2023/2854 arts. 23–27, 30, 35, especially arts. 25(2)(f), 30(6).

The W3C Verifiable Credentials Data Model 2.0 makes a useful distinction here: verification does not imply the truth of encoded claims, while verifier-side validation applies business rules to the propriety and fitness of a particular use. ABAC and XACML likewise demonstrate decision architectures in which current attributes and policies are evaluated at the point of use. OpenID Shared Signals Framework and CAEP demonstrate that cooperating receivers can react when previously relied-upon security state changes. These are implementation neighbors, not sources of substantive legal authority and not Paper 3 inventions.¹¹

The bounded contribution is to carry that discipline into persistent human–AI continuity. Legally material provenance should remain sufficiently connected to relevant state that the destination can determine the source of asserted authority, its scope, relevant lifecycle state, and any constraints that matter to the proposed operation. The destination then applies its own legal, institutional, and technical decision processes. The continuity layer is not the court, legislature, fiduciary, employer, regulator, or contracting party. It is the mechanism that avoids destroying the information those authorities need to remain meaningful after migration.

This residual is deliberately falsifiable. If mature generally applicable mechanisms already provide a sufficient cross-provider architecture for binding heterogeneous persistent relationship-state objects to their legally material authority sources, carrying lifecycle and contextual constraints interoperably, and producing destination-side legal-operability revalidation, then the residual should be narrowed further or closed. Paper 3 gains credibility by allowing that outcome rather than defending novelty as a goal.

7. INSTITUTIONAL AND THIRD-PARTY CONSTRAINTS

A person-centered continuity architecture encounters its hardest cases when the state is not solely about the person's private interaction with a consumer system. Workplaces, healthcare settings, financial institutions, schools, professional relationships, families, and collaborative environments generate information in which several actors can have legitimate interests. The fact that a piece of information becomes useful to one person's AI relationship does not dissolve those interests.

Trade-secret and confidentiality law provide a concrete example of why personal access and personal continuity do not imply exclusive legal control. Under Texas and federal trade-secret law, a person may lawfully encounter, remember, or technically possess protected information while remaining restricted in later use, disclosure, copying, downloading, uploading, transmitting, or transfer because the information is owned or protected by another party or subject to duties of secrecy or limited use. At the same time, the Texas statutory definition of a trade secret and its injunction provisions do not convert everything learned in employment into protected secret information or authorize restraint

¹¹ W3C, Verifiable Credentials Data Model v2.0 §§ 7.1 & app. A (Recommendation, May 15, 2025); NIST SP 800-162 § 2; OASIS XACML Version 3.0 § 1.1.1 & Administration and Delegation Profile Version 1.0 §§ 2–4; OpenID Foundation, OpenID Shared Signals Framework Specification 1.0 and OpenID Continuous Access Evaluation Profile 1.0 (Final Specifications, Aug. 29, 2025).

of employment merely because a worker acquired knowledge on the job.¹² That statutory boundary prevents the opposite overclaim that everything learned at work becomes employer-controlled. Persistent professional Relationship State can therefore contain both portable human capability and components that remain legally burdened by trade-secret, confidentiality, contractual, or third-party constraints.

The appropriate response is not to treat institutional custody as supremacy. Providers and institutions can be constrained by privacy, contract, fiduciary, consumer-protection, confidentiality, security, and sector-specific duties. Nor is the response to treat third-party presence as a universal veto. Minimization, redaction, selective disclosure, purpose limitation, access controls, and derived representations can support narrower uses where applicable law and institutional rules permit them; Paper 3 does not treat any of those mechanisms as automatically sufficient. The design requirement is to preserve enough provenance to know that a constraint exists and enough structure to avoid converting personal access into unconstrained downstream disclosure.

This reinforces the value of derived views in Paper 2—narrower assertions, summaries, preferences, constraints, or decisions whose provenance and permitted purpose can be represented without transporting the entire source object. A destination model may not need the original record to receive the continuity benefit. Paper 3 does not establish when such a transformation is legally sufficient. It establishes why the continuity architecture should be capable of making the distinction rather than assuming that usefulness requires wholesale replication.

8. DELEGATION, AUTOMATION, AND ACTION AUTHORITY

Persistent state becomes more consequential when AI systems move from advising to acting. An assistant may draft a message, schedule an appointment, submit a form, purchase a service, interact with another agent, or execute a workflow. At that point, the system must distinguish several questions that ordinary conversational interfaces can make look identical: who authenticated, who supplied information, who granted permission, who is being represented, what authority was delegated, and what action is legally attributable to whom.

Electronic validity and substantive authority are different legal questions. Texas UETA recognizes electronic records and signatures and permits contracts to be formed through electronic agents without contemporaneous human review, but it separately asks whether an electronic record or signature was the act of the person to whom it is attributed and then determines the legal effect of that attributed act from context, agreement, and other applicable law.¹³ Federal E-SIGN follows the same architecture: participation by an electronic agent does not by itself defeat legal effect, but the agent's action must be legally attributable to the person to be bound, while substantive rights and obligations remain governed

¹² Tex. Civ. Prac. & Rem. Code §§ 134A.002(6), 134A.003; 18 U.S.C. §§ 1832–1836, 1838.

¹³ Tex. Bus. & Com. Code §§ 322.005, 322.007, 322.009, 322.014.

by other law.¹⁴ Electronic execution, attribution, authentication, delegation, capacity, and substantive authority therefore should not be collapsed into a single authorization state.

Texas UETA makes attribution itself a layered inquiry. A security procedure can be evidence that an electronic record, signature, or performance was a particular person's act, but attribution does not by itself determine the legal effect of that act.¹⁵ The Act also requires agreement to conduct covered transactions electronically and makes clear that agreement to one electronic transaction does not necessarily extend to later transactions.¹⁶ A technically valid signature mechanism, credential, authentication event, stored preference, or prior workflow therefore cannot safely be treated as a universal authority token. The architecture needs to keep identity and attribution evidence distinguishable from capacity, delegation, scope, and the informational state that helps an agent perform an action.

Texas UETA expressly permits contract formation through interactions between electronic agents even when no individual knew of or reviewed the agents' actions or resulting terms, while providing that the terms of the resulting contract are determined by applicable substantive law.¹⁷ Its machine-mediated error rules likewise prescribe consequences in defined circumstances and return other errors to applicable law, including mistake doctrine and the parties' contract.¹⁸ Automation can therefore be legally effective and can alter the applicable legal analysis without becoming the independent source of substantive authority. This distinction becomes increasingly important as agents interact with agents: the receiving system needs more than confidence that the sending mechanism is authentic; it needs an adequate basis for determining what the relevant person or principal is legally entitled to request or cause.

9. INCAPACITY, SUPPORT, AND SUBSTITUTE AUTHORITY

Incapacity tests whether a continuity architecture is genuinely person-centered or merely account-centered. A person may have years of accumulated state when illness, injury, disability, or another legal circumstance changes who can make particular decisions. The account, credentials, and historical preferences may remain available. The authority to act may not.

Existing law already provides mechanisms such as powers of attorney, guardianship, fiduciary appointments, and forms of supported decision-making. Their scopes are not identical, and they do not make every representative the universal controller of the person's affairs. Under the Texas authorities used here, a supporter can assist without displacing the adult's decision-making authority; a limited guardianship order must specify the guardian's powers, limitations, or duties and the rights and powers

¹⁴ 15 U.S.C. §§ 7001, 7006.

¹⁵ Tex. Bus. & Com. Code §§ 322.002(13), 322.009.

¹⁶ Tex. Bus. & Com. Code § 322.005.

¹⁷ Tex. Bus. & Com. Code § 322.014.

¹⁸ Tex. Bus. & Com. Code § 322.010.

retained by the person; and an agent's authority can be limited by the instrument, statute, fiduciary duty, revocation, or other lifecycle events.¹⁹

For persistent AI continuity, the design implication is straightforward but demanding. The system should represent who is acting, under what external authority, for which domain or operation, and during what period. It should also preserve the distinction between historical knowledge about the person and present authority to use that knowledge. A representative may need access to information necessary for an authorized decision without gaining unrestricted access to every intimate conversation or machine inference accumulated over years.

That is another reason selective and derived views matter. The goal should not be to hand the entire relationship to whoever gains technical control of an account. The goal should be to make legitimate substitute authority usable while preserving boundaries that remain legally and institutionally meaningful. Paper 3 does not attempt to resolve contested capacity determinations. It argues that continuity architecture should be capable of reflecting the results of those external determinations without turning them into universal control.

10. DEATH, SUCCESSION, AND POST-MORTEM CONTINUITY

Death does not create a single legal rule for persistent digital state. Texas's Revised Uniform Fiduciary Access to Digital Assets Act differentiates among categories of digital assets and among the legal predicates governing post-mortem disclosure. A user's prior direction can control or prohibit disclosure, the fiduciary's authority remains bounded by applicable law and fiduciary duties, and federal communications law can independently constrain access to protected communications.²⁰

The distinction between communications content and other digital assets is particularly important. Under Texas law, disclosure of the contents of a deceased user's electronic communications to a personal representative requires a statutory route that includes user consent or a court direction, supporting documentation, and in some circumstances a court finding addressing the Stored Communications Act or other applicable law. By contrast, a communications catalog and many other qualifying digital assets follow a different disclosure rule unless the user prohibited disclosure or a court directs otherwise.²¹ The legal treatment of a persistent AI continuity package therefore cannot be inferred merely from the fact that all of its components were stored in one account.

The statute also resists a wholesale-transfer model in other ways. A fiduciary receives no new or expanded rights beyond those held by the user; authority remains subject to applicable terms of service, other law, and fiduciary duties. A custodian can in defined circumstances provide full account access, partial access sufficient for the fiduciary's task, or a copy of qualifying digital assets, and need not disclose assets the user deleted. Texas also excludes an employer's digital asset used by an employee in

¹⁹ Tex. Est. Code §§ 751.031, 751.131–.134, 1101.101, 1101.152, 1106.005, 1151.351, 1357.002, 1357.052.

²⁰ Tex. Est. Code §§ 2001.003, 2001.051–.053, 2001.101–.102, 2001.201, 2001.231; 18 U.S.C. § 2702.

²¹ Tex. Est. Code §§ 2001.101–.102.

the ordinary course of the employer's business from the Act's coverage.²² These distinctions reinforce a central Paper 3 proposition: a technically surviving account or record does not establish universal inheritable access, and personal association with state does not erase institutional boundaries.

Federal communications law adds another layer. Where a provider and the relevant material fall within the Stored Communications Act's coverage, the statute generally restricts voluntary disclosure of covered communications content, subject to enumerated exceptions including disclosure with the lawful consent of specified parties. The SCA example concerns disclosure or divulgence of covered communications; it is not offered as a general rule governing a provider's own internal operational use of retained content. Paper 3 relies on that statutory structure rather than a nonbinding state-court analogue for its bounded point: post-mortem access to protected communications is not established merely by death, family relationship, account possession, or technical persistence.²³

For human–AI continuity, the safe conclusion is therefore narrower than treating Relationship State as a single inheritable asset. A continuity archive may contain communications content, account data, machine inferences, locally stored state, provider-generated metadata, employer material, third-party information, credentials, and records of delegated actions. RUFADAA and the SCA do not necessarily classify all of those objects in the same way. Post-mortem operability should be evaluated component by component from the applicable legal predicates rather than inferred from persistence, possession, family relationship, or provider custody. This is the architectural reason to preserve provenance and state classification across succession: without them, a receiving fiduciary or system cannot reliably know which rules govern which part of the surviving continuity.

11. RETAINED-BUT-NON-OPERATIVE STATE

The distinction between retention and use appears throughout the preceding transitions. Texas privacy law supplies one bounded example without establishing a universal retention rule. Chapter 541 gives consumers a deletion right over covered personal data provided by or obtained about them, while separately preserving specified processing and retention grounds and permitting constrained compliance mechanisms for certain data obtained from other sources. The statute therefore does not make a deletion request synonymous with physical eradication of every related record.²⁴ At the same time, continued lawful retention does not itself establish authority for every other use; separate, domain-specific preservation, record-retention, and restriction regimes illustrate that distinction within their own scopes.²⁵

AI systems create a particular risk because retained information can remain computationally available. A record placed in an archive for compliance may still be retrievable by a model or agent

²² Tex. Est. Code §§ 2001.003, 2001.052–.053, 2001.201.

²³ 18 U.S.C. § 2702(a), (b)(3).

²⁴ Tex. Bus. & Com. Code §§ 541.051(b)(3), 541.052(f), 541.202, 541.204.

²⁵ Illustrative, domain-specific authorities: Fed. R. Civ. P. 26(b)(5)(B), 37(e); 17 C.F.R. § 240.17a-4; Regulation (EU) 2016/679 art. 18.

unless the architecture distinguishes storage from operative use. The same problem arises when a person corrects an inference. Preserving the prior inference for provenance can be valuable, but allowing it to continue shaping the current representation defeats the correction.

Retained-but-non-operative state is therefore an architectural condition in which the record survives for a legitimate historical, legal, audit, or evidentiary purpose while its ordinary authority to affect current interaction has been removed or narrowed. This condition should be represented explicitly rather than approximated through informal prompts such as 'ignore this from now on.' The appropriate implementation could involve policy, access controls, data-layer separation, derived views, credential status, or other mature mechanisms.

The concept should not be used to justify unnecessary retention. Data minimization, security, deletion rights, contractual duties, and sector-specific rules continue to apply. The point is narrower: where legitimate retention and current use diverge, continuity systems need to preserve that divergence rather than treating stored information as perpetually operative context.

12. REMEDIES, AUDITABILITY, AND CONTESTABILITY

Authority matters after the fact as well as before an operation occurs. If a continuity system discloses information to the wrong recipient, carries an expired delegation into a new provider, continues using a corrected inference, or permits an agent to act beyond its authority, the affected person or institution needs some way to discover what happened and invoke whatever existing remedy applies.

Law already supplies many remedy structures through contract, privacy statutes, fiduciary duties, consumer protection, regulatory enforcement, employment law, professional duties, and other doctrines. Texas Chapter 541, for example, requires a controller-side appeal process for denied consumer requests and provides a route to the Texas Attorney General complaint mechanism; the audited statutory layer reports Attorney General enforcement rather than a private right of action under the chapter. Paper 3 does not propose a new cause of action. Its architectural concern is whether cross-provider continuity preserves the evidence necessary for existing rights and remedies to remain usable.²⁶

That requires more than a generic activity log. A consequential operation may need provenance connecting the state used, the asserted authority, the actor or agent, the destination, the operation performed, the relevant policy decision, and subsequent corrections or revocations. The exact audit record will vary by system and legal domain. What matters is that migration should not sever the chain needed to understand why an action was permitted and whether the underlying authority was still operative.

²⁶ Tex. Bus. & Com. Code §§ 541.052(c), 541.053, 541.151–.156. Compare 15 U.S.C. § 45(a)(1), (n); Regulation (EU) 2016/679 arts. 77–83 (separate federal and EU remedial regimes).

Contestability also constrains machine inference. Relationship State can include inferred material, but an inference should remain distinguishable from a human statement or authoritative external record. If a machine-generated characterization becomes consequential, the person should be able to identify its status, inspect relevant provenance where appropriate, correct factual inputs, and contest continued reliance under whatever rights or processes apply. Paper 3 does not assert a universal legal entitlement to every form of explanation. It treats legibility and provenance as design features that make existing governance and remedy mechanisms more effective.

13. WHAT EXISTING LAW AND STANDARDS ALREADY SOLVE

Existing technical and legal mechanisms materially narrow the paper's contribution. Contextual authorization is not new. Attribute-based access control already evaluates authorization against subject, object, operation, environment, and policy. Policy administration, decision, enforcement, obligations, and delegated policy authority are not new. XACML and related systems provide mature architectures for them. Portable assertions with issuer provenance, validity periods, revocation or suspension status, selective disclosure, and verifier-side evaluation are not new. Verifiable Credentials provide a mature framework. Continuous signaling that prior access assumptions have changed is not new. Shared Signals and CAEP address that problem in identity and security contexts.²⁷

The same is true on the legal and institutional side. Consent, delegation, fiduciary authority, guardianship, digital succession, mandatory retention, electronic agents, complaint processes, contractual remedies, privacy rights, and provider switching all have mature legal or institutional antecedents. The EU Data Act goes particularly far in formalizing switching duties for covered data-processing services.²⁸ A credible Paper 3 must treat these mechanisms as the shelf from which a continuity architecture should build, not as inventions waiting for an AI label.

This anti-novelty posture changes the question. Instead of asking whether AI requires an entirely new law of memory or a new property right in relationship state, the paper asks whether the existing parts remain coherent when persistent state crosses boundaries. The answer from the current research is largely yes at the level of individual mechanisms. The residual appears in coordination: the state can move more easily than the legal and institutional context that made a particular use legitimate.

That result is useful even if later research closes the residual further. It means the first design obligation is not to invent a new governance regime. It is to preserve the information needed for mature regimes to keep working. The burden of proof therefore falls on any proposal for a new right, protocol, or legal category. Paper 3 does not currently meet that burden and does not need to do so to make its narrower contribution.

²⁷ See *supra* notes 5, 8, 11 (collecting the ABAC/XACML, Verifiable Credentials, and Shared Signals/CAEP sources for the mechanisms named in this paragraph).

²⁸ Regulation (EU) 2023/2854 arts. 23–27, 30, 35.

14. THE NARROW RESIDUAL COORDINATION PROBLEM

The residual can now be stated precisely. Persistent human–AI relationship state can contain heterogeneous objects governed by different authority sources and different incidents of use, disclosure, correction, restriction, retention, delegation, migration, and action. When those objects move across providers or contexts, the receiving environment can preserve their technical content while losing the legal and institutional information needed to determine whether prior authority remains operative.

The problem is not solved by attaching a single authorization flag to the package. Nor is it solved merely by signing the package, authenticating the sender, or verifying a credential. Those mechanisms can establish important facts, but legal operability can still depend on purpose, recipient, role, jurisdiction, time, third-party interests, institutional duties, and intervening lifecycle events. A destination needs enough legally material provenance to place the technical evidence back into the context in which a lawful decision can be made.

This does not require one universal schema. A continuity system might use policy engines, credentials, claims, event streams, records metadata, contractual controls, data-layer restrictions, or combinations of these mechanisms. The requirement is functional: do not erase the pedigree and current state of authority when moving the relationship state that authority governs. Where the source cannot establish destination operability, the transfer should preserve uncertainty rather than convert it into permission.

The residual is therefore best understood as a coordination problem between continuity and authority. The comparative review identified mature mechanisms for contextual authorization, credential validation, switching, retention, delegation, and lifecycle signaling, but did not establish a single generally applicable mechanism that binds heterogeneous persistent human–AI relationship-state objects to their external legal authority sources, carries all legally relevant lifecycle constraints across provider boundaries, and determines destination legal operability. This is a bounded comparative conclusion, not a claim that no such architecture exists, and the paper does not advance stronger novelty language.

15. IMPLICATIONS FOR PAPER 2 AND THE OPERANT DYAD SERIES

Paper 3 does not replace the first two papers. It supplies a missing constraint. Paper 1 describes the Operant Dyad and Relationship State as features of persistent, correction-shaped human–AI interaction. That description does not require Relationship State to become property, a legal person, or a new rights-bearing category. Paper 3 preserves that boundary.

Paper 2 asks how selected consequential state might persist across replaceable models and providers through provenance, temporal validity, correction, selective views, interoperability, and human governance. Paper 3 clarifies that a phrase such as authorized derived view cannot safely mean

'authorized everywhere.' Authorization must remain relative to an external source, a particular operation and object, current scope, relevant context, and the receiving environment's evaluation. This is a dependency clarification, not an automatic rewrite of Paper 2.

Several non-collapse findings follow. Technical portability is not lawful portability. Source authority is not destination authority. Retention is not operative use. A guardian is not a universal controller. A supporter is not automatically a substitute decision-maker. Third-party presence is not a universal veto. Automation is not legal authority. Provider custody is not provider supremacy. Person-centeredness is not exclusive personal legal control. These distinctions keep the Permanent Primitive principle from becoming an ownership slogan and make it more useful as an architectural constraint.

Taken together, the three papers describe different layers of the same problem. Persistent interaction produces relationship state. Governed continuity determines how selected state can remain useful without provider captivity. Authority determines whether and how that state may legitimately be used as circumstances change. The layers interact, but collapsing them would make each weaker: descriptive persistence does not establish technical portability, technical portability does not establish lawful use, and lawful authority cannot be manufactured by the continuity mechanism that represents it.

16. JURISDICTIONAL AND METHODOLOGICAL LIMITATIONS

This paper is intentionally bounded. The primary legal baseline is United States law, with federal law addressed where applicable and Texas used only as an illustrative state-law layer for privacy, agency, electronic transactions, guardianship, incapacity, succession, and digital assets. Texas also now has an AI-specific statutory overlay: the Texas Responsible Artificial Intelligence Governance Act (TRAIGA), effective January 1, 2026 and codified principally in Business & Commerce Code chapters 551–554. TRAIGA is included here as part of the jurisdictional baseline, not as a general rule governing portability, provenance, or authority transfer. The Texas authorities are not offered as uniform national law. European Union law is used selectively where GDPR or the Data Act materially sharpens correction, restriction, portability, switching, remedies, or cross-jurisdictional questions. The paper is not a fifty-state survey, a global comparative study, or an exhaustive treatment of every regulated sector.

The research record has a provenance limitation. Some underlying project research had to be reconstructed from preserved project materials during the August 2026 build; reconstructed material was treated only as a recovery aid and not as independent legal authority. Legal propositions in this article are supported by separately verified statutes, regulations, cases, orders, or official materials identified in the footnotes.

Source and authority discipline is proposition-specific. Legal claims were narrowed or removed where verified authority required it, technical standards received a bounded source/version check, and the publication footnotes identify the authorities relied upon. Citation or pinpoint corrections may improve source form but do not authorize broader propositions.

The paper's contribution is deliberately narrow. It offers a legal-institutional synthesis and configuration requirement, not a new legal doctrine, property category, cause of action, authorization method, portability rule, or technical primitive. The comparative treatment is illustrative rather than exhaustive, and the paper does not claim novelty beyond the bounded coordination problem described here.

17. CONCLUSION

Persistent human–AI continuity creates value because useful state can outlast a session, model, application, or provider. The same persistence creates a governance problem because legal authority does not necessarily follow the state with equal durability. A preference can remain recorded after a delegation expires. A fact can remain true after disclosure becomes restricted. A record can remain legally retained after ordinary use should stop. A technically portable package can arrive at a destination where only some of its components remain usable for the intended purpose.

Existing law and standards already solve much of the underlying machinery. They provide contextual authorization, policy evaluation, credential provenance, revocation, selective disclosure, delegation, fiduciary structures, succession rules, retention duties, switching mechanisms, auditability, and remedies. The appropriate response is therefore not to declare a new universal ownership right in relationship state or invent authority inside the continuity system. It is to configure continuity so those mature mechanisms are not stripped of their meaning when state moves.

That requires a simple but consequential discipline: preserve legally material provenance and authority lifecycle information with the state for which they matter, and require the receiving environment to evaluate current operability rather than inherit a context-free authorization status. The exact implementation can vary. What should not vary is the distinction between remembering something and being entitled to use it.

For the Operant Dyad series, that distinction completes an important separation of layers. Relationship State describes what can accumulate. Governed continuity describes how selected state can persist without provider captivity. Paper 3 adds the authority boundary: persistence can preserve the relationship's useful history, but the machinery that preserves it does not get to decide, by itself, what anyone is legally entitled to do next.

PRIMARY LEGAL AUTHORITIES

Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), (n).
 Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001, 7006.
 Stored Communications Act, 18 U.S.C. § 2702.
 Defend Trade Secrets Act, 18 U.S.C. §§ 1832–1836, 1838.
 Federal Rules of Civil Procedure 26(b)(5)(B), 37(e).

Exchange Act Rule 17a-4, 17 C.F.R. § 240.17a-4.

Texas Business & Commerce Code ch. 322 (Uniform Electronic Transactions Act).

Texas Business & Commerce Code ch. 541 (Texas Data Privacy and Security Act).

Texas Responsible Artificial Intelligence Governance Act (TRAIGA), Tex. Bus. & Com. Code chs. 551–554 (effective Jan. 1, 2026).

Texas Civil Practice & Remedies Code ch. 134A (Texas Uniform Trade Secrets Act).

Texas Estates Code chs. 751, 1101, 1357, 2001.

Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 15–22, 77–83.

Regulation (EU) 2023/2854 (Data Act), arts. 23–31, 35, especially arts. 25(2)(f), 30(6).

TECHNICAL AND STANDARDS SOURCES

National Institute of Standards and Technology (NIST). NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Jan. 2014; updates through 2 Aug. 2019).

OASIS. eXtensible Access Control Markup Language (XACML) Version 3.0, OASIS Standard, 22 Jan. 2013; XACML v3.0 Administration and Delegation Profile Version 1.0, Committee Specification Draft 04 / Public Review Draft 02, 13 Nov. 2014.

World Wide Web Consortium (W3C). Verifiable Credentials Data Model v2.0, W3C Recommendation, 15 May 2025.

OpenID Foundation. OpenID Shared Signals Framework Specification 1.0, Final Specification, 29 Aug. 2025; OpenID Continuous Access Evaluation Profile 1.0, Final Specification, 29 Aug. 2025; CAEP Interoperability Profile 1.0 — draft 01, 21 July 2026.