

GOVERNING RELATIONSHIP STATE

A Legal Framework for Human-Controlled AI Continuity

Operant Dyad — Paper 4

Micheal Preble

Independent Researcher

ORCID: 0009-0005-3906-6028

September 1, 2026

ABSTRACT

Persistent human–AI interaction can produce accumulated Relationship State: corrections, preferences, contextual interpretations, prior decisions, working methods, restrictions, authority representations, and other state that shapes later interaction. Existing law already governs many incidents of that state through privacy, data protection, contract, agency, consumer protection, records management, confidentiality, trade-secret law, and sector-specific regulation. The unresolved problem is narrower. Information can remain available, portable, and historically accurate after the factual, legal, institutional, or authority predicate that once justified consequential reliance upon it has changed.

This Article argues that the relevant legal object is not ownership of artificial-intelligence memory but lawful continuing reliance on persistent state. It proposes a purpose-limited governance interest for persons materially represented, affected, or used as a source of authority within Covered Relationship State. The proposed interest would support proportionate duties of visibility, contestability, provenance, Revalidation, restriction, Retirement from operative use, transition review, and protection against Material Reconstitution of previously invalidated state. Those duties would attach principally to actors possessing Legally Relevant Control Over Reliance rather than automatically to the original technical custodian.

The proposal does not assume that all consent is revocable, all state should be deleted, all derivatives can be traced, or all persistent state requires recurring authorization. Existing authority demonstrates instead that legal validity can expire, change, become disputed, require renewed verification, or cease to support future use while the underlying record remains. The paper develops an event-triggered and consequence-sensitive framework for addressing that condition while preserving lawful records, institutional memory, third-party rights, security, intellectual property, trade secrets, independent legal authority, and prior lawful reliance. The central claim is narrow: persistence, transfer, or technical reconstruction should not by themselves establish continuing authority for Consequential Reliance.

KEYWORDS

human–AI interaction; Relationship State; AI continuity; legal authority; provenance; Revalidation; portability; provider switching; artificial intelligence governance; data protection; contestability; Operant Dyad

1. CONTINUITY CAN OUTLIVE AUTHORITY

Persistent artificial-intelligence systems increasingly carry aspects of an ongoing working relationship forward. Corrections made in one interaction can influence later responses. Preferences can persist. Systems can retain contextual interpretations, prior decisions, institutional information, restrictions, and representations that make later interaction more useful because the relationship does not repeatedly begin from zero. Earlier papers in the Operant Dyad series describe this accumulated material as Relationship State and examine why continuity becomes valuable when applications, models, and providers remain replaceable.

Persistence creates a distinct legal problem when the state survives longer than the circumstances that made reliance upon it legitimate. An employee may have authority to approve a procedure while occupying one role and later move to another. A person may grant an authorization for a defined purpose and later revoke it where the governing law permits revocation. A factual representation may be corrected while a classification derived from it remains active. State may transfer successfully from one provider to another even though the destination operates under different contracts, institutional rules, purposes, or legal duties.

As developed in Paper 3, technical persistence does not establish continuing legal authority. Paper 3 argued that ownership is too coarse a master variable, that technical portability is not lawful portability, and that source-side authority should not be treated as a context-free status that automatically survives migration. Its contribution was architectural: legally material provenance and authority-state information should remain sufficiently connected to consequential continuity state that a receiving environment can reevaluate current legal operability. It expressly characterized that contribution as a synthesis and configuration requirement rather than a new legal right, ownership regime, or authorization primitive.¹

Paper 4 begins at that stopping point. It asks what prospective legal responsibility should follow when persistent state continues to be used after the validity of a material predicate has changed. The difference is between identifying an authority problem and allocating rights, duties, triggers, limits, and remedies around continuing reliance.

Current law already contains important pieces of this problem. Privacy and data-protection law govern access, correction, deletion, restriction, and portability. Agency law recognizes that actual and apparent authority can change. Authorization regimes recognize expiration and revocation. Consumer-reporting law provides dispute and reinsertion procedures. Records law sometimes requires historical information to remain preserved. European law increasingly regulates switching between data-processing services. Those legal forms substantially narrow any legitimate claim of novelty.

The remaining question is whether persistent human–AI systems can create a recurring coordination failure when they preserve state more reliably than they preserve the changing legal significance of that state. The same record can remain true as history while becoming an inadequate basis for present action. The same information can remain technically usable while a role, purpose, delegation, factual predicate, or legal condition changes. This Article does not purport to establish how frequently that condition occurs in deployed systems; it identifies a legally significant failure mode that can arise when persistent state and the predicates governing reliance evolve on different timelines.

This Article therefore asks: What legal and institutional framework should govern the continued use, transfer, restriction, Revalidation, Retirement, and Material Reconstitution of persistent Relationship State? Its central argument is that the relevant legal object is lawful continuing reliance. Where Covered Relationship State is used consequentially, the actor with Legally Relevant Control Over Reliance should bear proportionate duties to determine whether Material Predicates of present validity remain sufficient for the proposed use. Persistence alone should not answer that question. The analysis uses U.S. and EU authorities comparatively and synthetically; it does not claim a harmonized transnational rule. The proposed framework is a model governance architecture whose adoption, territorial scope, and enforcement would depend on jurisdiction-specific legal vehicles.

¹ Micheal Preble, *Authority Does Not Travel by Default: Legal Provenance and Revalidation in Persistent Human–AI Continuity*, Operant Dyad—Paper 3 (Aug. 26, 2026) (manuscript).

2. RELATIONSHIP STATE AS A PROBLEM OF RELIANCE, NOT OWNERSHIP

Ownership offers an intuitively simple model for persistent AI state. If the state belongs to the person, access, correction, portability, deletion, and control might appear to follow from a single rule. Existing information law generally does not operate that way. Legal systems routinely separate access from ownership, correction from title, confidentiality from destruction, portability from unrestricted transfer, and consent from every other possible legal basis for action.

Relationship State makes that separation especially important because the state can be heterogeneous. It may contain direct human statements, provider-generated metadata, institutional records, third-party information, machine-generated characterizations, preferences, corrections, permissions, restrictions, and historical records. Different components can be governed by different legal interests simultaneously. Paper 3 therefore rejected ownership as the master variable for authority analysis rather than rejecting ownership concepts where they otherwise apply.²

For purposes of this Article, Covered Relationship State means Relationship State materially used to characterize, coordinate with, attribute authority to, or make consequential decisions concerning a person or persistent human–AI relationship. The definition does not attempt to transform the broader Operant Dyad concept into a universal legal category. It identifies only the subset relevant to the governance framework developed here.

Within that category, Authority-Bearing State means Covered Relationship State relied upon as evidence of permission, consent, delegation, approval, restriction, role, legal capacity, institutional authority, or another predicate material to whether a present action is permitted. Authority-Bearing State can remain historically accurate after its legal significance changes. The record that an employee approved Version 3 last year may remain completely true even if the employee no longer possesses authority to approve Version 7 today.

This produces a foundational distinction between historical validity and current operative validity. Historical validity asks whether a representation was true or authorized at the relevant earlier time. Current operative validity asks whether that representation remains an adequate basis for Consequential Reliance now. Treating those questions as identical forces systems either to erase useful history or to treat historical authority as perpetual authority.

Consequential Reliance means use of Covered Relationship State in a manner reasonably capable of materially affecting legal rights, access, obligations, employment, financial interests, safety, institutional decisions, or another comparably significant interest. A remembered preference for concise responses ordinarily raises a different governance problem from a remembered delegation authorizing financial action or an inferred classification used in an employment decision.

The proposed legal framework therefore does not attach its strongest duties to every persistent representation. The case for intervention increases when persistent state materially represents a person, reflects that person's participation or authority, and is then used in a consequential setting. The relevant inquiry is not simply who possesses the technical state. It is whether the actor proposing Consequential Reliance has a sufficient current basis for doing so.

² *Id.*

3. WHAT EXISTING LAW ALREADY GOVERNS

Any proposal for a new governance framework should begin by subtracting the protections that already exist. This is especially important in AI governance, where familiar legal operations are often redescribed as if technical novelty had made the legal concepts themselves new.

Under current EU law, Article 18 of the GDPR permits restriction of processing in defined circumstances and expressly separates storage from other processing: restricted personal data may continue to be stored while further use is generally limited to specified grounds. Article 19 requires controllers to communicate qualifying rectification, erasure, or restriction to recipients unless doing so proves impossible or involves disproportionate effort. These provisions demonstrate both that retention and use can be legally separated and that corrections can produce bounded downstream obligations.³

Article 20 separately creates a defined portability right for qualifying personal data rather than a general property right over all information associated with an individual. The existence of separate access, correction, restriction, deletion, and portability rules itself counsels against treating Relationship State as a unitary object governed by a single incident of ownership.⁴

American law provides comparable domain-specific structures. Under current law, the Fair Credit Reporting Act requires a consumer reporting agency to conduct a reasonable reinvestigation of qualifying disputed information. If the information is inaccurate, incomplete, or cannot be verified, the agency must modify or delete it. Information deleted under that process cannot simply be reinserted unless the furnisher certifies that it is complete and accurate; reinsertion also triggers notice, and agencies must maintain reasonable procedures designed to prevent unauthorized reappearance.⁵

As a structural analogue, the FCRA demonstrates that law can distinguish possession of information from eligibility to restore that information to an operative decision environment, and can require a validating event before previously removed information regains practical effect. It does not directly govern persistent human–AI Relationship State.

Federal records law demonstrates the opposite side of the problem. Under current law, agency heads must preserve adequate documentation of agency organization, functions, policies, decisions, procedures, and essential transactions, including information necessary to protect governmental and individual legal and financial rights.⁶ The requirement shows why a governance framework cannot assume that deletion is always the appropriate response when authority or factual status changes. Some records must survive precisely because they document what occurred.

Authorization law supplies another useful comparator. Under 45 C.F.R. § 164.508, a HIPAA authorization must contain an expiration date or expiration event, and the regulation identifies circumstances in which an authorization is defective, including when the covered entity knows that the expiration event has occurred or that the authorization has been revoked. The regulation also recognizes that revocation generally does not unwind action already taken in reliance on a previously valid authorization.⁷ As a structural analogue, this

3 General Data Protection Regulation arts. 18–19, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

4 *Id.* art. 20.

5 15 U.S.C. § 1681i(a)(1), (a)(5)(A)–(C).

6 44 U.S.C. § 3101.

7 45 C.F.R. § 164.508(b)(2)(v), (b)(5) (2026).

framework shows that authorization can have a lifecycle independent of the persistence of the underlying information.

Consent law likewise resists simplification. As a structural analogue, *Van Patten v. Vertical Fitness Group, LLC* treated the scope of TCPA consent as dependent on the transactional context in which it was given and recognized revocation through a sufficiently clear expression.⁸ By contrast, *Reyes v. Lincoln Automotive Financial Services* held that TCPA consent incorporated into the bargained-for terms of a binding contract could not be unilaterally revoked under the rule applied there.⁹ These cases do not establish a Relationship-State rule. They show why the proposal must distinguish legally revocable consent from contractual, statutory, institutional, and other forms of authority.

Agency law offers another analogy. As a structural analogue, *Herbert Construction Co. v. Continental Insurance Co.* applied New York apparent-authority principles requiring principal-created manifestations and reasonable reliance, and explained circumstances in which a third party has reason to know that earlier authority has terminated.¹⁰ The case does not establish an AI-state rule; it illustrates a more general legal instinct that earlier evidence of authority does not remain indefinitely self-validating.

The Data Act supplies a mature comparator for technical and contractual switching. Under current EU law, Article 23 requires covered providers to remove specified obstacles to switching and supports porting of exportable data and digital assets. The Regulation does not, however, impose the same functional-equivalence obligation across every service model; Recital 86 expressly limits that facilitation obligation to providers offering the IaaS delivery model. The switching regime therefore demonstrates legal regulation of technical transition without establishing a general transfer of source-side authority.¹¹

Treaty-body interpretation similarly suggests an information-governance baseline without creating a Relationship-State right. Human Rights Committee General Comment No. 16 interprets ICCPR Article 17 to call for legal regulation of the gathering and holding of personal information and describes the ability to ascertain stored personal data and seek rectification or elimination of incorrect or unlawfully processed

8 *Van Patten v. Vertical Fitness Group, LLC*, 847 F.3d 1037, 1045–48 (9th Cir. 2017) (treating the scope of TCPA consent as dependent on transactional context and requiring revocation to clearly express a desire to stop further calls or texts).

9 *Reyes v. Lincoln Automotive Financial Services*, 861 F.3d 51, 56–59 (2d Cir. 2017) (holding, under the TCPA rule applied there, that consent incorporated into a bargained-for contract could not be unilaterally revoked). The case is cited here only as a limitation on any universal revocation proposition. The FCC has since codified TCPA revocation by reasonable means and prohibited callers from designating an exclusive revocation method, while expressly declining to resolve the intersection of the TCPA and negotiated contractual revocation terms and observing that courts remain equipped to apply relevant contract law. See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 39 FCC Rcd 1988, paras. 10, 15 & n.33 (2024). A January 2026 FCC order extended until January 31, 2027 only the portion of 47 C.F.R. § 64.1200(a)(10) that would apply a revocation concerning one type of informational message to unrelated future robocalls and robotexts. See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, DA 26-12, paras. 1, 6, 10, 12 (CGB Jan. 6, 2026).

10 *Herbert Construction Co. v. Continental Insurance Co.*, 931 F.2d 989, 993–96 (2d Cir. 1991) (applying New York apparent-authority principles and analyzing reasonable reliance where surrounding circumstances may require further inquiry).

11 Data Act arts. 23–24, recital 86, Regulation (EU) 2023/2854, OJ L, 2023/2854, 22.12.2023. Recital 86 limits the obligation to facilitate functional equivalence to providers offering the IaaS delivery model.

information.¹² It is interpretive material, not domestic legislation or a direct command governing persistent AI continuity.

Taken together, these authorities significantly constrain Paper 4. Ordinary access, correction, restriction, deletion, portability, records preservation, dispute procedures, and downstream notification are not new merely because a persistent AI system is involved. The residual claim must begin after those protections have been recognized.

4. THE RESIDUAL GAP: WHEN INFORMATION REMAINS BUT ITS BASIS FOR RELIANCE CHANGES

The residual problem is not an absence of law governing information. It is the possibility that persistent systems preserve a representation while the predicate that once made Consequential Reliance on that representation legitimate changes independently.

A role can end while the system still remembers it. An authorization can expire while the authorization record remains. A factual representation can be corrected while a derived eligibility classification continues to influence later decisions. A provider can receive a technically valid state package without receiving certainty that every source-specific permission remains operative for the destination's purpose.

For purposes of this Article, a Material Predicate is a fact, authority, role, purpose, consent, provenance element, legal condition, or other circumstance whose validity matters materially to whether Consequential Reliance is presently justified. Material Predicates are not assumed to behave alike. Their creation, modification, expiration, and revocability remain governed by the substantive law that creates them.

The coordination problem arises because state and predicate can move on different timelines. Persistent systems are intentionally designed to reduce repeated reconsideration of prior context. That is part of their value. Yet the same design can create a failure mode if the system remembers the earlier representation while losing sight of the fact that its operative authority was conditional.

Four categories illustrate the gap. Authority changes when a delegation, appointment, approval, or role ends. Permission changes when a legally revocable authorization is withdrawn or a use exceeds the scope of the governing permission. Factual status changes when information is corrected, disputed, or becomes unverifiable. Context changes when the provider, institution, recipient, purpose, or relationship differs materially from the environment in which the state was accumulated.

None of those changes necessarily invalidates the underlying historical record. The legal question is whether they create a reason to reconsider present reliance. The target is therefore not old data in the abstract or a general right to control memory. It is stale validity: the assumption that persistence itself establishes that a Material Predicate remains sufficient for current consequential use.

5. A PURPOSE-LIMITED RELATIONSHIP-STATE GOVERNANCE INTEREST

Identifying a residual gap does not itself justify a new legal interest. Law frequently tolerates overlapping doctrines and fragmented institutional responsibility. This Article therefore proposes only the smallest legal form necessary to address the coordination problem identified above: a purpose-limited governance interest in Covered Relationship State.

12 Human Rights Comm., General Comment No. 16: Article 17 (Right to Privacy), ¶ 10, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (Apr. 8, 1988). This is treaty-body interpretation, not domestic legislation or a freestanding Relationship-State right.

The proposed interest is procedural and functional rather than proprietary. It does not make a person owner of the database, model, institutional record, inference system, employer information, or every mixed-origin representation generated through a persistent relationship. Instead, it recognizes a legally relevant interest where state materially represents a person, materially reflects that person's participation or authority, and is then used in a consequential setting.

Four factors help identify the strength of the interest. Representation asks whether the state purports to characterize the person. Participation asks whether the state materially incorporates the person's decisions, corrections, instructions, or sustained interaction. Authority asks whether the state is used as evidence of permission, delegation, approval, or restriction derived from that person. Consequence asks whether the state is being used in a manner capable of materially affecting legal or comparably important interests.

The proposed governance interest would support specific operations rather than absolute dominion. Depending on context, those operations could include visibility into material state being relied upon, meaningful contestability, correction where existing or proposed law permits it, access to material provenance, proportionate Revalidation of changing predicates, prospective recognition of legally effective revocation, Retirement of historical state from ordinary current use, and safeguards when affected state transfers or undergoes Material Reconstitution.

This framework also preserves mixed-origin interests. A persistent state item may simultaneously implicate the person, another participant, an employer, a provider, an institution, or a third party. Governance should therefore follow legally cognizable interests, provenance, and function rather than presumed unitary ownership. One participant may possess a strong interest in correcting a false attribution without possessing a right to erase another participant's lawful statement or an institution's required record.

The corresponding duty should not attach permanently to whoever first stored the state. Responsibility should follow the actor that possesses Legally Relevant Control Over Reliance. That actor may be a provider in one context and an employer, institution, professional user, or downstream decision-maker in another.

This Article proposes that a person materially represented, affected, or used as a source of authority within Covered Relationship State should possess governance protections sufficient to prevent Consequential Reliance on materially inaccurate, improperly attributed, expired, effectively revoked, out-of-scope, or unvalidated state, subject to competing legal interests, lawful records requirements, independent legal authority, and proportionate implementation constraints. The most important operational consequence of that interest is Revalidation.

6. REVALIDATION

Revalidation means a process sufficient under the circumstances to determine whether a Material Predicate supporting proposed Consequential Reliance remains valid after a material change or legally significant uncertainty. It is broader than consent. Consent is only one possible predicate among identity, role, delegation, factual status, institutional authority, purpose, source, or another condition necessary for legitimate use.

Existing law already demonstrates several forms of event-triggered validity review. As structural analogues, apparent-authority doctrine can make continued reliance depend on whether belief in authority remains reasonable after later events; HIPAA authorization rules explicitly recognize expiration events and known revocation; and the FCRA requires new certification before information removed after reinvestigation

can be reinserted.¹³ These regimes do not collectively establish a general Relationship-State Revalidation duty. They show that requiring renewed verification after a material event is a familiar legal structure.

This Article proposes an event-triggered and consequence-sensitive Revalidation duty. It should arise when an actor with Legally Relevant Control Over Reliance knows, or under defined circumstances reasonably should recognize, that a Material Predicate necessary to the proposed Consequential Reliance may no longer be valid. The rule should not impose strict liability for facts an actor could not reasonably know and had no reason to investigate.

Some triggers are comparatively strong. A legally effective revocation, expiration of an authorization, termination of a delegation, loss of an institutional role, successful material correction, or failed verification can directly call continued reliance into question. Other events are more contextual. A provider change or new purpose should matter only when the change bears materially on the predicate supporting the consequential use.

Elapsed time alone should ordinarily be weak evidence. Some state remains useful for years. A stable preference should not require recurring confirmation merely because it is old. Time becomes relevant when the underlying authority is time-limited, role-dependent, context-dependent, or when intervening events create a reasonable basis for doubt.

The form of Revalidation should vary with consequence. Where no material change exists, no new action should be necessary. Moderate uncertainty may require a lightweight verification of role, identity, source, or status. High-consequence reliance after a material authority change may require renewed delegation, institutional confirmation, source certification, renewed consent where consent is actually the governing revocable basis, or another appropriate validating event.

If a Material Predicate cannot presently be validated, deletion should not be automatic. The historical state may remain important or legally required. The appropriate disposition may instead be restriction or Retirement from ordinary Consequential Reliance.

The standard should also separate future reliance from prior lawful action. HIPAA's treatment of revocation illustrates the logic: later revocation does not necessarily undo actions already taken in reliance on a valid authorization.¹⁴ The proposed framework is primarily concerned with what happens after a material change, not with retroactively rewriting lawful history.

This Article proposes the following rule: when an actor with Legally Relevant Control Over Reliance knows, or reasonably should recognize, that a Material Predicate necessary to Consequential Reliance has materially changed, expired, been effectively revoked, become credibly disputed, or cannot presently be verified, the actor should undertake proportionate Revalidation before continuing or restoring that reliance unless an independent lawful basis makes the affected predicate unnecessary.

13 See *Herbert Construction Co. v. Continental Insurance Co.*, 931 F.2d 989, 993–96 (2d Cir. 1991); 45 C.F.R. § 164.508(b)(2)(v), (b)(5) (2026); 15 U.S.C. § 1681i(a)(5)(B)–(C). These authorities are structural analogues and do not establish a general Relationship-State Revalidation duty.

14 45 C.F.R. § 164.508(b)(5) (2026).

7. RETIREMENT: PRESERVING HISTORY WITHOUT PRESERVING OPERATIVE AUTHORITY

Revalidation sometimes confirms that state remains usable. In other cases the relevant predicate has expired, been revoked, or failed verification. Persistent systems then need an outcome other than unrestricted use or deletion.

This Article uses Retirement to mean preservation of Covered Relationship State where lawful or required while removing or materially limiting its ordinary eligibility to support current Consequential Reliance. The concept is the prospective legal treatment of the retained-but-non-operative condition identified architecturally in Paper 3.¹⁵

As structural analogues, GDPR Article 18 expressly allows storage to continue while other processing is restricted, while federal records law can affirmatively require preservation of historical documentation.¹⁶ Neither body of law creates a general Relationship-State Retirement doctrine, but together they demonstrate why legal preservation and present operational use should not be collapsed.

Consider an employee who validly approved a procedure while holding a role. The historical approval may need to remain because it explains earlier actions. If the employee leaves the role, deleting the approval could damage the record; treating the approval as continuing current authority would distort it. Retirement preserves the truthful history while changing its operative status.

Retirement should also ordinarily preserve the possibility of lawful reinstatement. A delegation may be renewed, a dispute resolved, or new current authority established. What should be prevented is not reinstatement after valid reauthorization, but silent reinstatement based solely on persistence.

The proposed rule is therefore that where Covered Relationship State remains lawfully preserved but a Material Predicate necessary for ordinary Consequential Reliance has expired, been effectively revoked, materially changed, or failed Revalidation, the responsible actor should be capable of retiring that state from ordinary Consequential Reliance while preserving the historical record and any independent lawful uses that remain.

8. TRANSFER AND PROVIDER TRANSITION: PORTABILITY WITHOUT TRANSITIVE AUTHORITY

Portability can preserve the value of persistent interaction across replaceable systems. It can also create a legal shortcut if successful transfer is treated as proof that every source-side permission or authority remains valid at the destination.

Under current law, the GDPR provides a defined portability right in specified circumstances. The Data Act separately requires covered data-processing-service providers to remove specified switching obstacles and supports porting of exportable data and digital assets. The Regulation does not impose the same functional-equivalence obligation across every service model; Recital 86 limits that facilitation obligation to IaaS providers.¹⁷ These regimes regulate movement and transition. They do not establish that every source-side authority predicate becomes operative at the destination.

¹⁵ Preble, *supra* note 1. Paper 3 describes retained-but-non-operative state as an architectural condition rather than an existing legal category.

¹⁶ General Data Protection Regulation art. 18, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1; 44 U.S.C. § 3101. These authorities are structural analogues for separating preservation from operative use.

This Article therefore proposes portability without transitive authority. A legal or technical entitlement to transfer Relationship State should not, without an independent basis, be treated as transferring every authority, permission, delegation, purpose limitation, or institutional predicate under which the source environment previously relied on the state.

The rule does not mean every transfer requires fresh consent or formal review. Many items can move without raising any material authority question. The stronger obligation arises where the destination intends to use Authority-Bearing State consequentially and the relevant Material Predicate may depend on the source context.

Destination responsibility should remain reasonableness-based. A destination provider cannot reconstruct unknowable upstream history. But an express restriction, expiration indicator, dispute, Retirement status, source-specific role, or material contextual change can create a basis for further review. Missing authority information should not automatically become affirmative proof of continuing authority merely because the state arrived successfully.

Source and destination responsibilities should also remain distinct. A source actor may have duties not to strip known restrictions or materially misrepresent exported state. A destination actor that adopts the state for a new consequential use may have an independent duty to assess current operability. Responsibility therefore follows function rather than a permanent assumption that the original custodian remains responsible for every later use.

9. MATERIAL RECONSTITUTION

State does not need to be directly transferred in order to return. A representation that has been corrected, restricted, retired, or otherwise removed from ordinary Consequential Reliance can later be recreated from summaries, exported information, conversation history, organizational records, or derivative state. The technical object may be different while the practical consequence becomes substantially the same.

As a structural analogue, the FCRA's reinsertion regime conditions the return of information deleted after reinvestigation on furnisher certification, requires notice after reinsertion, and requires reasonable procedures designed to prevent unauthorized reappearance.¹⁸ The statute does not govern AI reconstruction, but it demonstrates that restoration after invalidation can itself be treated as a legally significant event.

This Article proposes the term Material Reconstitution for restoration or recreation of substantially equivalent operative state where the recreated state materially depends upon previously corrected, restricted, effectively revoked, retired, or otherwise invalidated state and would restore substantially the same Consequential Reliance.

The definition deliberately requires more than similarity. A destination that independently reaches the same conclusion from new, current, valid evidence has not necessarily reconstituted the earlier state. A person can receive a new delegation equivalent to an old one. A corrected factual conclusion can later become accurate because circumstances changed. Regulation of mere semantic similarity would be unworkable and overbroad.

17 General Data Protection Regulation art. 20, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1; Data Act arts. 23–24, recital 86, Regulation (EU) 2023/2854, OJ L, 2023/2854, 22.12.2023.

18 15 U.S.C. § 1681i(a)(5)(B)–(C). The FCRA directly governs consumer reporting, not persistent human–AI Relationship State.

Two requirements therefore control the analysis. First, there must be material dependency on the affected earlier state or a reasonably traceable derivative. Second, there must be restored operative effect: the recreated state must again support substantially the consequential use that the earlier correction, restriction, revocation, or Retirement had limited.

An employee example illustrates the distinction. If a terminated delegation remains in historical records and a replacement system uses those records to explain an earlier transaction, no present authority has been restored. If the replacement system infers from those records that the employee is still authorized and allows a current transaction on that basis, the historical state has effectively re-entered the operative decision environment.

Proposal, not current law: when Material Reconstitution restores state that is again used for Consequential Reliance, the actor with Legally Relevant Control Over Reliance should conduct renewed review when the predicates that formerly justified that reliance have been invalidated, expired, materially disputed, superseded, or retired.¹⁹ The purpose of the gate is not permanent suppression. It is to ensure that technical recreation does not itself function as proof that earlier invalidity has disappeared.

10. CORRECTIONS, REVOCATIONS, AND DEPENDENT STATE

Material Reconstitution addresses state that returns. A related problem arises when an earlier predicate has already shaped later classifications, summaries, workflow rules, recommendations, or other state.

Under current law, GDPR Article 19 requires communication of qualifying corrections, erasures, or restrictions to recipients subject to impossibility and disproportionate-effort limitations. The FCRA links dispute, reinvestigation, modification, deletion, furnisher notice, and later reporting.²⁰ These regimes support bounded downstream governance structures; neither establishes a general derivative-state rule for AI systems.

The residual issue concerns dependent state, not merely copied records. Suppose an erroneous certification record causes a system to classify an employee as ineligible for assignments. Correcting the source record may accomplish little if the classification remains active solely because the system never revisits it. The same problem arises when a terminated delegation remains embedded in a derived workflow rule.

Universal propagation would be disproportionate and often technically impossible. This Article therefore proposes a bounded test requiring three conditions: material dependency, reasonable traceability, and Consequential Reliance.

Material dependency requires that the downstream state materially depend on the affected predicate rather than merely share historical association. Reasonable traceability means that the dependency can be identified through information and capabilities reasonably available to the relevant actor; the framework does not require reconstruction of a perfect causal graph. Consequential Reliance limits the strongest duty to uses capable of materially affecting significant interests.

Even when the test is satisfied, deletion is not the presumptive remedy. Appropriate outcomes can include correction, qualification, dispute notation, restriction, Revalidation, Retirement, downstream notice, or no change where independent current evidence adequately supports the later state.

19 Cf. 15 U.S.C. § 1681i(a)(5)(B)–(C) (conditioning reinsertion of deleted consumer-report information on certification and requiring notice); 45 C.F.R. § 164.508(b)(5) (2026) (recognizing revocation while preserving specified prior reliance). The proposed Material Reconstitution rule is an analogy-based governance design; neither authority directly regulates persistent human–AI Relationship State.

20 General Data Protection Regulation art. 19, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1; 15 U.S.C. § 1681i.

The proposed rule therefore requires proportionate review of downstream state where a legally significant change affects a Material Predicate on which that state materially depends, the dependency remains reasonably traceable, and continued Consequential Reliance could reproduce the affected consequence.

11. DUTY BEARERS AND FUNCTIONAL CONTESTABILITY

Persistent state can pass through several actors before producing a consequential result. The original provider may store the state, another provider may receive it, an employer may deploy the destination system, and a manager may control the final decision. A legal framework that assigns every duty permanently to the first custodian fails when Consequential Reliance moves downstream. A framework that makes every technical intermediary fully responsible is equally unworkable.

Legally Relevant Control Over Reliance means sufficient decision-making or institutional control to determine, authorize, continue, suspend, or materially alter the Consequential Reliance at issue. The term identifies the principal duty bearer without assuming that custody alone determines responsibility.

Different roles can carry different duties. A state custodian may owe security, correction, retention, or provenance obligations. A transferor may be responsible for faithful transmission of known restrictions. A destination provider may be responsible for imported state it chooses to use consequentially. A deploying employer or institution may control the substantive decision and therefore bear the principal Revalidation obligation. Shared responsibility does not require identical responsibility.

The proposed framework also requires functional contestability. A person materially affected by Consequential Reliance should have a meaningful way to challenge the material basis of that reliance. This is broader than ordinary factual correction but narrower than a right to inspect every proprietary computation.

Two challenges should be distinguished. An accuracy challenge asserts that the representation is factually wrong, incomplete, or misleading. An authority challenge accepts that the representation may be historically correct but contests its eligibility to support the current use. 'I never approved this' and 'I approved this two years ago, but that approval no longer authorizes this action' are different claims.

Meaningful contestability should therefore provide enough functional information to identify the material state being relied upon, relevant source or provenance, purpose, known dispute or restriction status, and the path for correction, Revalidation, or review. It should not presumptively require source code, model weights, internal architecture, proprietary algorithms, or other protected implementation details.

The question is whether the affected person can challenge the legally significant reliance, not whether the person can inspect the entire system.

12. LIMITS, COMPETING INTERESTS, AND INSTITUTIONAL MEMORY

Human governance cannot mean unilateral control over every artifact associated with a persistent relationship. The proposed interest must coexist with recordkeeping duties, prior lawful reliance, independent legal authority, third-party rights, intellectual property, trade secrets, confidentiality, security, public responsibilities, and technical proportionality.

Records provide the clearest example. Under current law, federal agencies may be legally required to preserve documentation of decisions and essential transactions.²¹ A person whose authority later changes

²¹ 44 U.S.C. § 3101.

cannot acquire a general power to erase that record. The stronger governance claim is that preservation should not automatically preserve current operative authority.

The same reasoning applies to prior lawful reliance. A later revocation or expiration should ordinarily govern future use rather than automatically rewrite actions that were authorized when taken. The historical record and the present authority status can coexist.

An independent lawful basis can also survive the loss of another predicate. If consent expires but a separate legal obligation independently requires an action, the proper response is not to pretend consent remains valid. The system should identify the actual present basis on which Consequential Reliance proceeds.

Third-party rights require the same incident-specific approach. A person can possess a strong interest in correcting a false representation concerning themselves without acquiring ownership of another person's information or an institution's record. A portability or visibility right may therefore require redaction, separation, limitation, or alternative review where another protected interest is implicated.

Trade-secret law reinforces the boundary. Under current law, federal trade-secret protection requires qualifying information, reasonable measures to maintain secrecy, and independent economic value from secrecy.²² That protection can legitimately limit disclosure of proprietary implementation. It does not automatically establish that a consequential decision based on persistent state is immune from correction, authority review, or functional contestability.

Security, professional secrecy, privilege, investigations, and public duties can likewise constrain disclosure or portability. The limiting principle should be operation-specific: an exception should restrict the governance operation with which it genuinely conflicts rather than automatically extinguishing the entire governance interest.

Technical proportionality matters as well. The framework should not demand perfect lineage or impossible reconstruction of every computational influence. At the same time, an actor should not be able to avoid foreseeable governance obligations merely by designing a consequential system so that no relevant provenance, correction status, or authority state can ever be recovered. The appropriate position lies between perfect reversibility and deliberate ungovernability.

13. REMEDIES AND ENFORCEMENT

The appropriate remedy should correspond to the governance failure. A missing explanation is different from an inaccurate fact. An inaccurate fact is different from expired authority. Expired authority is different from improper restoration of previously retired state.

Visibility and provenance failures ordinarily call first for informational remedies: disclosure of the material state relied upon, relevant source information, current purpose, known restriction status, and available challenge process. Accuracy failures can require reinvestigation, correction, qualification, dispute notation, or bounded review of dependent state.

Authority failures should ordinarily be repaired at the authority level. If a historical representation is accurate but present authority is uncertain, the presumptive response is Revalidation or temporary non-reliance, not alteration of the historical record. An effective revocation or expiration can require prospective restriction or Retirement where the affected predicate was necessary and no independent lawful basis exists.

²² 18 U.S.C. § 1839(3).

Improper Material Reconstitution may justify suspension of the restored state, renewed Revalidation, restoration of a prior dispute or Retirement status, and notice where appropriate. As a structural analogue, the FCRA reinsertion structure demonstrates why restoration can legitimately carry procedural consequences beyond ordinary correction.²³

Persistent-state governance particularly favors prospective and injunctive remedies because the central problem is continuing reliance. Preventing obsolete authority from influencing tomorrow's decision may be more useful than compensating for the problem only after repeated use.

Damages should nevertheless remain a separate inquiry. A governance duty can be violated without establishing every element necessary for compensable injury. Any future statutory regime would need to determine the appropriate relationship among actual injury, causation, materiality, fault, statutory damages, regulatory penalties, and private enforcement. This Article therefore does not propose automatic damages for every procedural defect.

A useful remedial ladder runs from information and correction through Revalidation, restriction, Retirement, controlled reinstatement, injunctive or administrative orders, and finally monetary remedies where independently justified. The ladder is not an exhaustion requirement; serious conduct may justify immediate stronger intervention. Its purpose is to ensure that the legal framework contains more precise responses than the binary alternatives of unrestricted use and litigation for damages.

Institutionally, the proposal does not yet require a single regulator or comprehensive new statute. A general set of minimum reliance-governance principles could operate through existing sectoral structures where those structures can implement them adequately. Broader legislation would require a further showing that fragmentation leaves recurring gaps that sector-specific law cannot manage efficiently.

14. COUNTERARGUMENTS

The strongest objection is that existing law may already be sufficient. Privacy, agency, contract, employment, consumer-protection, records, and sector-specific regimes can address many harms produced by persistent state. The proposal should fail if it merely duplicates those protections under new terminology.

The response is necessarily conditional. Where current law already supplies an equivalent access, correction, Revalidation, restriction, or contestability duty, the proposed framework adds nothing. Its case is strongest only at the residual coordination point where existing doctrines govern separate predicates but no clear *ex ante* mechanism keeps those changing predicates synchronized with persistent state used across time, systems, or institutions.

A second objection is burden. Requiring systems to reconsider every remembered fact or preference would destroy the value of continuity. The proposal avoids that result by limiting Revalidation to material changes or legally significant uncertainty involving Consequential Reliance. Persistence itself is not a trigger.

A third objection is epistemic feasibility. A destination actor cannot know everything about a source environment, and complex AI systems cannot trace every derivative. That concern requires a reasonableness standard, not abandonment of governance. Duties should follow known or reasonably detectable changes, available provenance, material dependency, reasonable traceability, and consequence. Unknown history should not create strict liability, but neither should missing authority information automatically count as proof of continuing authority.

23 15 U.S.C. § 1681i(a)(5)(B)–(C).

Material Reconstitution raises a similar concern. Two systems can independently reach the same conclusion. The proposed rule therefore does not regulate similarity. Material Reconstitution requires both traceable material dependency and restoration of substantially the same consequential effect. Independent evidence or newly granted authority is outside the rule.

Institutional overlap remains the most important unresolved policy question. A broad federal statute could conflict with mature sector-specific systems. A model law or set of baseline principles implemented through existing regulators may prove more proportionate. This Article therefore establishes the governance problem and candidate legal operations without claiming that a single institutional vehicle has already been proven superior.

The surviving claim is smaller than a right to control AI memory. Persistent systems can preserve state longer than some of the predicates that made reliance upon it legitimate. Where consequential use depends on a predicate that materially changed, a bounded framework can require recognition of the change, proportionate Revalidation, preservation of lawful history without perpetual authority, and protection against materially dependent restoration of the affected consequence.

Whether that framework should ultimately be generalized across sectors depends on empirical prevalence, existing remedies, implementation cost, and the adequacy of sector-specific law. Those questions should constrain the policy recommendation rather than being obscured by the novelty of the technology.

15. RELATIONSHIP TO THE OPERANT DYAD

The four-paper sequence addresses different layers of the same persistent-interaction problem. Paper 1 identifies Relationship State as an accumulated feature of persistent human–AI interaction. Paper 2 asks how selected state can remain useful across replaceable providers and systems. Paper 3 establishes that persistence and portability do not automatically preserve the external legal authority governing use.²⁴

Paper 4 asks the prospective question that follows: when persistent state is used consequentially, what legal responsibility should attach to continuing reliance?

The sequence does not imply that Relationship State automatically receives a new legal status. The existence of the state does not prove ownership. Portability does not prove destination permission. Architectural Revalidation does not by itself prove that a new statutory right is necessary. The proposed governance interest must therefore stand or fall on the residual legal problem developed here.

The contribution of Paper 4 is to translate the authority constraint identified in Paper 3 into a candidate allocation of rights and duties around continuing reliance, Revalidation, Retirement, transition, Material Reconstitution, contestability, and remedies.

16. CONCLUSION: CONTINUITY SHOULD PRESERVE HISTORY WITHOUT FREEZING AUTHORITY

Persistent AI systems can preserve useful context across time. That capability can improve human–AI collaboration by carrying corrections, preferences, decisions, restrictions, and institutional knowledge forward rather than requiring constant reconstruction. As continuity becomes more durable and portable, however, historical state can remain computationally active after the factual, legal, or institutional predicate that once made reliance legitimate has changed.

²⁴ Preble, *supra* note 1.

Current law already governs much of this territory. Privacy and data-protection regimes provide access, correction, restriction, deletion, portability, and downstream notification. Agency and contract law govern different forms of authority. Authorization regimes recognize expiration and revocation. Consumer-reporting law provides dispute and reinsertion controls. Records law protects institutional memory. Trade-secret and confidentiality law protect competing interests. Provider-switching law increasingly governs technical transition. Those regimes make a sweeping new property theory unnecessary.

The narrower problem is continuing reliance. A record may remain true without remaining current authority. A delegation may remain documented after the role ends. A correction can be valid while dependent state still reproduces the original consequence. Transferred state can arrive technically intact while destination-side authority remains uncertain. Retired state can return through a different technical representation.

This Article proposes that where Covered Relationship State is used for Consequential Reliance, the actor with Legally Relevant Control Over Reliance should bear proportionate responsibility for determining whether Material Predicates necessary to the use remain valid. That responsibility becomes stronger when an express expiration, legally effective revocation, material correction, failed verification, significant contextual change, or attempted restoration creates a reason to question continuing validity.

The framework does not require constant consent or recurring confirmation of benign persistent state. It does not require universal deletion. It does not make every derivative traceable by legal fiction. It does not override institutional records, third-party rights, security, confidentiality, trade secrets, public duties, or independent legal authority.

Its central operations are correspondingly limited. Revalidation addresses changing predicates. Retirement preserves history while removing ordinary operative authority. Portability without transitive authority separates technical transfer from destination permission. Bounded dependent-state review prevents materially traceable derivatives from silently reproducing a corrected defect. Material Reconstitution prevents technical recreation alone from restoring operative legitimacy that the underlying state had lost.

The governing principle is straightforward: a durable record can preserve what was once true without determining what remains authorized now. That distinction is familiar outside artificial intelligence. What persistent AI changes is the ease with which historical state can remain operational. A record in an archive is visibly different from an active instruction. In a computational continuity system, the same representation can remain available for retrieval, inference, ranking, personalization, or action unless the system and the institution controlling it can distinguish preservation from present authority.

The legal objective should not be to force persistent systems to forget whenever circumstances change. Forgetting can destroy evidence, accountability, useful continuity, and institutional memory. Nor should the objective be to force users to repeatedly authorize everything a system knows. That would defeat the practical value of continuity. The more precise objective is to make persistence governable.

A governed continuity system should be capable of remembering history without silently converting history into perpetual authority. It should be capable of carrying useful state across providers without assuming that permission is transitive. It should preserve disputes and corrections in forms that remain consequentially meaningful. Where materially dependent state reappears after correction, restriction, revocation, or Retirement, technical reconstruction should not itself supply the missing legal predicate.

Whether these principles ultimately belong in a federal statute, model legislation, sectoral regulation, contractual mandatory floors, or a hybrid framework remains an implementation question. Existing law may already provide adequate equivalents in some settings and should not be displaced merely for uniformity.

The narrower conclusion does not depend on resolving that question today. Lawful continuing reliance on persistent state is a distinct governance problem. Persistence, transfer, and reconstruction should preserve useful continuity, but none should silently manufacture current authority.

Persistent systems should be permitted to preserve useful history without treating memory as permanent authority. The legal objective is not forced forgetting, but governable continuity: state may persist while the authority supporting Consequential Reliance remains capable of changing, expiring, being disputed, or requiring renewed validation. Continuity should preserve history without freezing authority.