

DANA

SOVEREIGN

Infrastructure for Collective Data Leverage

Working Paper, Second Edition

Second edition, May 2026. Revised September 2026.

dana.xyz

Abstract

For twenty years, the power dynamic between platforms and the people who generate their data has been determined not by law, not by rights frameworks, and not by consumer choice — but by architecture. Platforms built systems where data, once given, could not be meaningfully revoked. The result was structural leverage: the platform held the data and set the terms.

Regulatory responses — GDPR, CCPA, and their descendants — addressed the symptom (consent) without changing the underlying structure (access). Individual opt-outs do not create negotiating power. They create friction that platforms route around.

This paper argues that data sovereignty is an architecture problem, not a policy problem. It describes SOVEREIGN, an infrastructure pattern where data access is revocable, time-bounded, and collective — where the platform has to negotiate instead of extract. The architecture supplies a commitment and coordination technology rather than a guarantee of cooperation. Section 4 states the four conditions under which fair terms are sustainable, and Section 5 the scope limit that follows: the argument closes for differentiated institutional data and does not close for commodity consumer data.

The second edition includes deployment guidance — what an organization needs in place, what the architecture gives it, and what it does not — and Section 5 tests the argument against the record: a decade of failed individual data markets, the structural objection that individualist mechanisms cannot price relational data, the collective-licensing regimes that solved this shape of problem, the prices currently being set without the data's source in the room, and the condition that would falsify the whole thesis.

1. The Problem

Architecture Creates Leverage

Every digital platform operates on a simple premise: collect data, then use that data to create value. The question is who captures that value. For the past two decades, the answer has been the platform — not because of superior negotiation, but because the architecture made negotiation unnecessary.

When a user uploads data to a platform, the platform copies it into systems the user cannot see, cannot audit, and cannot revoke access to. The data becomes an asset of the platform. The user retains a legal right — in theory — but no structural power. The architecture is the leverage.

Why Regulation Has Not Changed the Dynamic

The GDPR, adopted in 2016 and applicable from May 2018, was the most ambitious attempt to rebalance data power through law. It established the right to access, the right to erasure, the right to portability. Eight years later the bargaining dynamic is substantially unchanged, and the measured effect on market structure ran the wrong way: Johnson, Shriver and Goldberg (2023) find GDPR increased web-technology vendor concentration by

roughly 17% in the short run, with the gains accruing to the largest incumbents. GDPR did reduce data sharing. It did not redistribute bargaining power, and it entrenched the firms best able to absorb compliance cost.

This is not a failure of enforcement. It is a failure of mechanism design. The GDPR gives individuals the right to withdraw consent. But individual withdrawal is not a credible threat to a platform serving hundreds of millions. One user leaving changes nothing. The platform's architecture does not require any single user's continued participation.

The result is a rights framework that is technically enforceable but structurally irrelevant. The right to delete your data does not give you the power to negotiate the terms under which your data is used.

The Collective Action Gap

If individual withdrawal has no leverage, what about collective withdrawal? In labor markets, this problem was solved centuries ago: unions aggregate individual power into collective bargaining. But data markets have no equivalent mechanism.

The reason is architectural rather than conceptual. Collective structures for data already exist — data cooperatives (Hardjono and Pentland 2019), bottom-up data trusts (Delacroix and Lawrence 2019), and since 2022 a legal category for them in the EU Data Governance Act's "data intermediation services." What does not exist is deployed technical infrastructure for coordinated, credible withdrawal. Users cannot jointly commit to revoking access. They cannot make time-bounded offers. They cannot condition access on terms. Every interaction is bilateral — one user, one platform — and bilateral interactions with asymmetric power always favor the party that can wait.

2. The Insight

Data sovereignty is not about who owns the data. It is about who controls the architecture through which data flows.

The core insight behind SOVEREIGN is that data leverage follows architecture, not law. If the architecture gives one party persistent, unconditional access to data, that party has leverage regardless of what the law says. If the architecture makes access conditional, revocable, and time-bounded, the party granting access has leverage regardless of their size.

This means data sovereignty is not a feature you add to an existing system. It is a property of the infrastructure itself. You do not make a platform sovereign by adding a consent banner. You make it sovereign by changing the conditions under which data is accessed.

Three Architectural Properties

SOVEREIGN infrastructure enforces three properties that, together, create structural leverage for data providers:

- Revocable access. Data access can be withdrawn at any time, and the next request is refused. Revocation is architectural for *future* access: the infrastructure enforces it at the boundary, on every read. It does not reach what has already been served, and the lessee's retention of what it received is governed by the lease, not by the infrastructure. Section 3 states the boundary precisely.

- Time-bounded access. Every data access grant has an expiration. There are no perpetual licenses. If the platform wants continued access, it must renew — which means it must offer terms worth renewing for.

- Collective access. Data providers can coordinate their access grants. A group can make a joint offer: access to all members' data on shared terms, or access to none. This is the mechanism that creates negotiating power.

No single property is sufficient. Revocability without time-bounding allows indefinite access as long as no one actively revokes. Time-bounding without collectivity still leaves each user negotiating alone. Collectivity without revocability is an empty threat. The three properties are load-bearing as a set.

3. The Architecture Pattern

SOVEREIGN does not prescribe a single implementation. It defines an infrastructure pattern that any organization can deploy. The pattern has four layers.

This pattern is a synthesis rather than an invention, and the antecedents should be named. Continuous, revocable, attribute-conditioned access is the UCON model (Park and Sandhu 2004). Machine-readable terms travelling with data are "sticky policies" (Pearson and Casassa Mont 2011) and, as a standard, W3C ODRL (2018). Personal datastores with app-mediated access are Solid (Mansour et al. 2016). Most directly, the International Data Spaces reference architecture (Otto et al. 2019) already ships connector-enforced, time-bounded, revocable usage policies with clearing-house audit logs across a large B2B deployment — Layers 1, 2 and 4 in production form.

What is not present in that prior art is a collective coordination layer specified as an infrastructure primitive sitting on top of usage-control enforcement, and that is this paper's contribution. The phrase "data leverage" in this paper's subtitle is Vincent, Li, Tilly, Chancellor and Hecht's (2021), whose framework establishes the public-leverage argument this architecture is built to serve.

Layer 1: The Access Envelope

Every data access request is wrapped in an access envelope that specifies the grantee, the scope, the duration, and the terms. The envelope is the atomic unit of data access. Nothing passes through the infrastructure without one.

An envelope is a machine-enforceable constraint over admission, and a contract over everything downstream of it. The distinction matters and the paper keeps it throughout.

Gate-enforced, with no grace period and no discretion: expiry, revocation, and scope. When the duration lapses the next request is refused; a request outside the envelope's scope is refused; a tampered envelope fails

signature verification.

Contract-enforced: purpose limitation, retention, and derivative use. Detecting that a lessee used data outside its permitted purpose is not something the boundary can observe — it requires audit, attestation, disclosure, or a watermark, on human timescales. An earlier edition claimed that access terminates when terms are violated. That claimed a violation-detection oracle this architecture does not provide. What it does provide is a signed, non-repudiable record of exactly what was granted, which turns an unprovable dispute into an evidentiary one.

Layer 2: The Revocation Layer

Revocation is a first-class infrastructure primitive, not a feature bolted onto an existing system. When a data provider revokes access, the next request is refused. Revocation is checked at the boundary on every read. At a single enforcement point it takes effect on the next request; across several, it takes effect within a stated freshness interval, which Section 6 records as a deployment parameter rather than an absolute.

It is important to be exact about what this does and does not reach, because the distinction is the difference between a security property and a marketing claim.

Revocation governs **future access**. It does not reach data already served. It does not reach a cache the lessee chose to keep, a copy it made, or — most consequentially — anything derived from the data: an embedding, an aggregate, a trained model. Deleting a retained copy does not undo what that copy produced. Once bytes have been read, cryptography has no further hold on them; what happens next is governed by the terms of the lease, which is to say by contract and by law.

The reference implementation (``apps/sovereign-poc``) states this in its test suite rather than in prose. Three tests assert the limitation and are designed to pass permanently: revocation does not reach data already served, derived artifacts survive revocation, and ``prohibitedUse`` is carried in the credential but never enforced at the boundary — it is a string the vault transmits and does not read.

An earlier edition of this paper claimed revocation propagates to every copy, derivative, and cache. That claim was wrong, and the implementation refutes it.

What follows from the true version is still substantial, and it is an admission-control property rather than a containment one: a platform that wants continued access must return, and the provider can decline. That is leverage. It is not erasure, and a system that promises erasure is promising something no architecture can deliver.

Layer 3: The Collective Coordination Layer

The coordination layer allows data providers to form groups with shared terms. A group publishes a single access offer: here is what we provide, here is what we require, here is when it expires. Platforms respond to the group, not to individuals.

Group formation is voluntary and non-exclusive. A provider can belong to multiple groups with different terms for different data types. The coordination layer handles the mechanics of group offers, acceptance, and enforcement. It does not dictate the terms — that is for the group to decide.

Layer 4: The Negotiation Interface

Platforms interact with SOVEREIGN infrastructure through a negotiation interface. The interface presents available data offers (individual and collective), accepts or rejects terms, and manages active access grants. It is the only path to data — there is no backdoor, no bulk export, no API that bypasses the envelope.

The negotiation interface changes the game theory. A platform that wants data from a SOVEREIGN network must offer terms that the providers — individually or collectively — find acceptable. The alternative is no access at all. This is not an ideological position. It is an architectural constraint.

4. Why This Works: The Game Theory

SOVEREIGN creates a repeated game with credible commitment. In the current architecture, data providers make a one-shot decision (share or don't share) with no ability to condition future access on platform behavior. This is a classic one-shot game where the platform has a dominant strategy of extraction.

SOVEREIGN converts this into a repeated game. Because access is time-bounded, the platform must return to negotiate at regular intervals. Because access is revocable, the data provider has a credible exit threat. Because coordination is possible, groups can make the exit threat collectively credible.

In repeated games with credible exit, cooperation can be sustained as *an* equilibrium — one of many the folk theorem admits, and only when discount factors are high enough that future access is worth more than present extraction (Fudenberg and Maskin 1986). It is not a dominant strategy, and an earlier edition of this paper said it was. The distinction matters: a dominant strategy is optimal whatever the other party does, which is plainly false here.

Two conditions have to hold, and neither is guaranteed by architecture. Defection must be observable — and Section 3 has just conceded that misuse after serving is not observable at the boundary. And withdrawal must be costly to the platform, which fails if it can substitute correlated data from non-members; Acemoglu, Makhdoumi, Malekian and Ozdaglar (2022) show that correlated data makes exactly this substitution cheap, and it is the reason individual withdrawal has no leverage in the first place. The same mechanism erodes a coalition's threat.

Olson (1965) supplies the third problem. The phrase "when the group is large enough" names the condition under which free-riding is hardest to prevent, not easiest.

What the architecture actually supplies is a commitment and coordination technology, not a cooperation machine. It removes hold-up, by deleting the platform's ability to expropriate raw data outside an envelope. It rebundles the trade, converting N negotiations over marginal-value data into one negotiation over an aggregate the platform cannot cheaply replicate. And at the joining stage its quorum-conditional commitment is genuinely sound: because signing costs nothing if the quorum fails, joining weakly dominates staying out — a provision-point mechanism (Bagnoli and Lipman 1989) laid over an assurance game. That is the one place in this paper where a dominance claim is legitimate, and it is not the claim the earlier edition made.

Fair terms are then a sustainable equilibrium provided four conditions hold, none of which architecture can guarantee:

- **Imperfect substitutability.** The platform's fallback — synthetic data, non-participants, inference from correlated members — must be worth materially less than the coalition's supply. Where a platform's own revealed marginal valuation of one person's data is a fraction of a cent, this condition fails.
- **Excludability and a defensible joining window. A platform can pay a blocking set to stay out. Note the perverse arithmetic: a higher quorum is safer for members but cheaper to block*,* since fewer holdouts defeat it.
- **A bounded ratchet.** Because revocation governs raw data at the boundary but trained derivatives only by contract, every completed lease permanently raises the platform's fallback. Leverage decays with each renewal unless model deletion or an ongoing royalty is part of every envelope.
- **Renewal bargaining that actually reprices.** Lease frequency sets how often terms can be reset. It does not set the split.

Scope: Where This Closes and Where It Does Not

These conditions are not evenly satisfied, and the honest consequence is a scope limit rather than a caveat.

For commodity consumer data the coalition is not stable. Providers are near-perfectly substitutable, the fair-terms allocation is not in the core, and the arrangement is a cartel held together by a commitment device rather than an equilibrium of the underlying market. The credible per-member gain is small.

For differentiated institutional data — a region's hospital systems, a media archive, a research consortium — substitutability is low, the number of suppliers is small, per-member stakes are large, and a quorum covering most relevant suppliers is organizationally achievable. This is where the model closes, and it is where the reference implementation is aimed. The Implications section names the same sectors. The game theory says they are not merely relevant there; they are the condition of the argument working at all.

5. What This Argument Has to Survive

A pattern that has not been tested against its own history is a proposal, not a paper. This section states the evidence for and against.

The Record of Individual Data Markets Is Uniformly Bad

Every attempt to pay individuals for their own data has failed in the same way. Datacoup launched in 2014 promising roughly \$8 per month and shut down in 2019. Swash still operates, but documented user earnings run to a few dollars over eighteen months, and the product has drifted toward paid surveys. Brave Rewards pays most users under a dollar a month, and it is an advertising revenue share rather than a price for data. Ocean Protocol abandoned the retail data-selling vision. California's proposed data dividend produced a single bill, AB 950, which would only have required disclosure of what data was worth; it died without passage.

The clearest statement came from the Streamr Data Union DAO, which paused fundraising in 2023 and said that the business case for dedicated data-union infrastructure had not been strong enough to attract venture capital. The demand side never appeared.

The market price is the reason. The Financial Times' data-broker calculator prices general demographic data at roughly \$0.0005 per person, with a complete profile under a dollar.

The Strongest Objection Is Structural, Not Empirical

In *A Relational Theory of Data Governance* (Yale Law Journal, 2021), Salomé Viljoen argues that data's value is population-level and relational — it arises from placing people into aggregate relations with one another — and that individualist mechanisms such as ownership, sale, or licensing therefore cannot capture or govern it at any price.

This paper concedes the argument as stated. An individual selling an individual profile is selling something worth a fraction of a cent, and no protocol changes that arithmetic.

It is also the reason the three properties in Section 2 are load-bearing as a set rather than individually. Revocability and time-bounding are enforcement primitives. They do not discover a price. Collective coordination is not the hardest of the three properties to build and therefore last — it is the one the other two exist to serve.

Collective Licensing Has Solved This Shape of Problem Repeatedly

A dispersed group, each member holding something individually near-worthless and collectively essential, facing a small number of well-capitalized buyers, is not a new situation.

SoundExchange distributed \$991.5 million in 2025 to more than 850,000 music creators. No artist negotiates with a streaming service. A compulsory license means services cannot refuse to pay, the Copyright Royalty Board sets the rate, and the split is fixed by statute. Holdouts are impossible in both directions.

The Mechanical Licensing Collective, created by the Music Modernization Act of 2018, has distributed over \$3.3 billion since 2021. Two design decisions transfer directly to this architecture: the licensees fund the collective's operating costs, so distributions are not skimmed; and royalties that cannot be matched to a person are pooled, published, and claimable — an answer to the question of what happens to people who never enrolled.

European private copying levies collect over one billion euros a year, charged to device manufacturers and importers rather than to individuals. There is no holdout problem because individuals are not asked to act.

The 2023 SAG-AFTRA agreement prices a digital likeness, requiring specific consent per project and compensation at scale minimums for use of a digital replica.

In each case the price was set collectively or judicially and enforced individually. The ordering is never reversed.

Prices Already Exist, Set by Parties That Exclude the Data's Source

In July 2026 a federal court gave final approval to a \$1.5 billion settlement covering more than 480,000 works used to train a model — roughly \$3,100 per work, set by a judge. In February 2024 a reported \$60 million per year was agreed for access to a social platform's archive; against that platform's reported 130.3 million daily active users, this is roughly forty-six cents per user per year; measured against weekly actives it is nearer twelve. For 2025, one large platform reported worldwide average revenue per person of \$57.03.

Four orders of magnitude separate these figures. What varies is not the data. It is whether the people who produced it had an instrument that made them a party to the negotiation.

The Consent Infrastructure Now Exists, Without a Price Attached

California's Deletion Request and Opt-Out Platform opened to consumers on 1 January 2026; more than 300,000 residents filed requests in its first months, and since 1 August 2026 over 600 registered data brokers must poll it every 45 days. The EU Data Act became applicable on 12 September 2025, obliging providers to remove barriers to porting and switching. India's DPDP framework creates a registered consent-manager role binding from 13 November 2026, although the board that must register them was not yet fully constituted as of August 2026.

These are consent rails without a meter. Revocation, portability, and intermediation have been built by regulators, and no price is attached to any of them. That gap is the specific opportunity this architecture addresses.

The Coordination Layer Has an Antitrust Problem

A group of independent suppliers agreeing on common terms and jointly withholding supply is, on its face, horizontal price-fixing combined with a concerted refusal to deal — per se unlawful under Sherman Act §1 and a restriction by object under Article 101 TFEU.

The precedent is directly on point. In *FTC v. Superior Court Trial Lawyers Ass'n*, 493 U.S. 411 (1990), independent contractors collectively withheld services until their fees were raised. The Supreme Court held the boycott per se illegal and held that the sympathetic purpose was irrelevant.

The collective licensing regimes cited above do not rescue the argument; read carefully, they complicate it. ASCAP and BMI are lawful **because their consent decrees make withholding impossible** — grants from members are non-exclusive, the organization must license any applicant on request, and a federal rate court sets the fee when negotiation fails. SoundExchange is lawful because 17 U.S.C. §114(e)(1) contains an express antitrust exemption, which Congress wrote even for collective negotiation over a compulsory license. These institutions bought their legality by surrendering exactly the credible exit threat Section 4 depends on.

That is a real tension in this paper and it is stated here rather than left for a referee.

Three things follow. First, single-organization deployment — one hospital system, one archive, governing its own data estate — raises no Section 1 question at all, and that is where the reference implementation sits. Second, multi-party collectives require a legal basis this architecture cannot supply: an express exemption on the §114(e) model, a compulsory license with an administrative rate backstop, or an extension of labour-law protection. US

doctrine currently runs the other way for independent sellers of a commodity (*Columbia River Packers v. Hinton*, 315 U.S. 143 (1942)). Third, the EU offers the nearest lawful lane: the Data Governance Act's "data cooperatives" (Art. 2(15)) create an institutional home for member-directed negotiation, though the Act's Art. 12 neutrality duties constrain what an intermediary may itself do, and it confers no antitrust immunity whatsoever.

An architecture cannot create the standing to bargain. It can only be ready for the moment standing exists.

What Would Falsify This

If a collectively set rate were introduced and platforms substituted synthetic or non-participating data at an acceptable quality cost, the leverage described in Section 4 evaporates and the argument fails. This is the condition to test before building the coordination layer, and it is approximately what happened to every data union that assumed a scarcity it did not have.

6. From Paper to Production

The second edition of this paper addresses a gap in the first: the distance between understanding the pattern and running it. SOVEREIGN infrastructure is designed to be deployable in stages rather than all at once. An organization with an existing data practice can stand up the lease boundary — signed, scoped, expiring, revocable access — before any of the coordination layer exists.

What You Need

- An existing data practice with identifiable data providers and consumers.
- Infrastructure that you control (cloud or on-premise). SOVEREIGN does not depend on any specific cloud provider.
- A decision about scope: which data types, which providers, which consumers.
- Engineering time. The reference implementation is partial: the lease boundary is demonstrated end to end, the coordination layer is specified but not built.

What You Get

- Machine-enforceable access envelopes for every data access request.
- Revocation enforced at the boundary on every read, and propagated to registered enforcement points within a stated freshness interval. Not real time, and not reaching copies already served — the interval is a deployment parameter and should be published as an SLA.
- The specification for the coordination layer. Not the layer itself — see "What You Need" above. An organization deploying today gets the lease boundary and builds group negotiation on top of it.
- A negotiation interface for the lease boundary — issuing, presenting and renewing envelopes. Group-level negotiation is specified, not built.

- Tamper-evident logs of every admission decision the boundary made. These prove what the gate did. They do not prove what a lessee did with data after it was served, and no log at this layer can.

What Changes

After deployment the relationship changes in one specific respect: a consumer can no longer obtain data without a current envelope, so continued supply requires returning to the provider. Data already served, and anything derived from it, remains with the consumer under the terms of the lease. Providers can refuse renewal individually, and collectively where the conditions in Section 4 hold. What the architecture requires is renegotiation; whether renegotiation produces better terms depends on the substitutability of the data, not on the software.

7. Implications

For Organizations

Organizations that deploy SOVEREIGN infrastructure gain two things: actual control over their data relationships, and a credible position in any negotiation with platforms. This is particularly relevant for organizations that produce high-value data — healthcare providers, financial institutions, research organizations, media companies — and have historically lacked the technical infrastructure to enforce the terms they want.

For Platforms

Platforms that engage with SOVEREIGN networks on fair terms gain access to data they would otherwise lose. As SOVEREIGN adoption grows, the platforms that cooperate early build relationships that non-cooperating platforms cannot replicate. First-mover advantage in SOVEREIGN cooperation is a strategic asset, not a concession.

For Regulators

SOVEREIGN infrastructure makes part of regulatory enforcement verifiable rather than aspirational. Access envelopes create auditable records of what was granted, to whom, under what terms, and for how long, and revocation at the boundary is provable. What becomes a property of the system is the record of admission decisions. Compliance with purpose limitation and retention terms remains a claim made by the lessee — the records make that claim contestable with evidence, which is a smaller thing than proof and a larger one than nothing.

8. Conclusion

Data sovereignty has been framed as a rights problem. It is an architecture problem. Rights without infrastructure are aspirational. Infrastructure without rights is extractive. SOVEREIGN combines both: it takes the principles embedded in modern data protection law and makes them architecturally enforceable.

The result is not a utopia where platforms and users hold hands, and it is not a structure that makes cooperation rational everywhere. It is a structure in which, where the supplied data is genuinely hard to substitute, refusal becomes possible and therefore terms become negotiable. Platforms get reliable, renewable access. Providers get a position from which to bargain — not a guaranteed price. Where the data is easily substituted, the architecture changes the paperwork and not the outcome, and Section 5 says so.

The architecture is specified, and the part that carries its central claim is demonstrated: access is admitted or refused cryptographically, and what happens to data after it is served is governed by contract, not by cryptography. Saying so plainly is what makes the rest of the argument worth having.

References

- Acemoglu, Daron, Ali Makhdoumi, Azarakhsh Malekian, and Asuman Ozdaglar. 2022. "Too Much Data: Prices and Inefficiencies in Data Markets." *American Economic Journal: Microeconomics* 14 (4): 218-56.
- Bagnoli, Mark, and Barton L. Lipman. 1989. "Provision of Public Goods: Fully Implementing the Core through Private Contributions." *Review of Economic Studies* 56 (4): 583-601.
- Delacroix, Sylvie, and Neil D. Lawrence. 2019. "Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance." *International Data Privacy Law* 9 (4): 236-52.
- Fudenberg, Drew, David M. Kreps, and Eric Maskin. 1990. "Repeated Games with Long-Run and Short-Run Players." *Review of Economic Studies* 57 (4): 555-73.
- Fudenberg, Drew, and Eric Maskin. 1986. "The Folk Theorem in Repeated Games with Discounting or with Incomplete Information." *Econometrica* 54 (3): 533-54.
- Hardjono, Thomas, and Alex Pentland. 2019. "Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management." arXiv:1905.08819.
- Johnson, Garrett A., Scott K. Shriver, and Samuel G. Goldberg. 2023. "Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR." *Management Science* 69 (10): 5695-721.
- Mansour, Essam, Andrei Vlad Sambra, Sandro Hawke, Maged Zereba, Sarven Capadisli, Abdurrahman Ghanem, Ashraf Abounaga, and Tim Berners-Lee. 2016. "A Demonstration of the Solid Platform for Social Web Applications." *WWW '16 Companion*, 223-26.
- Olson, Mancur. 1965. *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge, MA: Harvard University Press.
- Otto, Boris, Sebastian Steinbuss, Andreas Teuscher, and Steffen Lohmann. 2019. *IDS Reference Architecture Model, Version 3.0*. Berlin: International Data Spaces Association.
- Park, Jaehong, and Ravi Sandhu. 2004. "The UCON_ABC Usage Control Model." *ACM Transactions on Information and System Security* 7 (1): 128-74.

Pearson, Siani, and Marco Casassa Mont. 2011. "Sticky Policies: An Approach for Managing Privacy across Multiple Parties." *IEEE Computer* 44 (9): 60-68.

Viljoen, Salome. 2021. "A Relational Theory of Data Governance." *Yale Law Journal* 131 (2): 573-654.

Vincent, Nicholas, Hanlin Li, Nicole Tilly, Stevie Chancellor, and Brent Hecht. 2021. "Data Leverage: A Framework for Empowering the Public in Its Relationship with Technology Companies." *FAccT '21*, 215-27.

W3C. 2018. *ODRL Information Model 2.2*. W3C Recommendation, February 15, 2018.

Cases and instruments cited: *FTC v. Superior Court Trial Lawyers Ass'n*, 493 U.S. 411 (1990); *Columbia River Packers Ass'n v. Hinton*, 315 U.S. 143 (1942); *Broadcast Music, Inc. v. CBS*, 441 U.S. 1 (1979); 17 U.S.C. §§112, 114; Regulation (EU) 2016/679 (GDPR); Regulation (EU) 2022/868 (Data Governance Act); Regulation (EU) 2023/2854 (Data Act).

SOVEREIGN is a Dana venture. dana.xyz

Copyright 2026 Dana. All rights reserved.