International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 12-No.1 (2026) pp. 1366-1381
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

The Automotive Data-Equity Loop: Converting Telemetry into Consumer-Owned Resale Value Through Verifiable Digital Passports

Karishma Verma*

Independent Researcher, USA
* **Corresponding Author Email:** karishmakvermaa@gmail.com - **ORCID:** 0000-0002-0047-7877

Article Info:

DOI: 10.22399/ijcesen.5032
Received : 05 January 2026
Revised : 28 February 2026
Accepted : 10 March 2026

Keywords

Automotive Telemetry,
Verified Credentials,
Data Equity,
Consumer Privacy,
Behavioral Economics

Abstract:

The transformation of vehicles into software-defined platforms creates a fundamental trust gap between consumers and entities seeking detailed telemetry data. Traditional incentive models, including direct payments and feature personalization, fail to motivate sustained telemetric sharing because they cannot overcome consumer concerns about surveillance, fairness, and asymmetric value extraction. This article introduces the Automotive Data-Equity Loop, a socio-technical framework that reframes telemetry sharing from data extraction to asset protection by converting operational data into durable, consumer-owned verified credentials that enhance resale value. The framework operates through three interconnected phases: value creation during ordinary vehicle use, value crystallization through privacy-preserving conversion of raw telemetry into tamper-resistant cryptographic credentials, and value realization when verified history reduces buyer uncertainty in resale transactions. The hybrid asset conceptual model positions vehicles as composite assets integrating physical components with verifiable digital history layers, leveraging behavioral-economic principles, including loss aversion and endowment effects, to align long-term consumer interests with platform data requirements. The transparency slider interface operationalizes graduated consent through multi-level controls mapping sharing choices to certification outcomes, while purpose-bound certificates restrict secondary use by design. Comparative analysis establishes testable hypotheses predicting that asset value enhancement outperforms alternative incentive structures through increased perceived fairness and reduced exploitation concerns. The governance blueprint addresses multi-stakeholder trust through explicit role definitions for credential issuers, verifiers, and marketplace participants, alongside threat models addressing consumer gaming, forgery attacks, and marketplace pressure dynamics. Implementation requires empirical validation through controlled experiments measuring adoption rates, persistence duration, and depth of consent, complemented by observational market studies assessing effects on resale prices, transaction velocity, and buyer confidence indicators. The framework demonstrates how consumer-generated data ecosystems can align with autonomy and long-term value creation when systems treat individuals as asset owners rather than extractable data sources, with implications extending beyond automotive contexts to broader Internet of Things and smart asset domains.

1. Introduction and the Trust Gap in Software-Defined Vehicles

The car market is experiencing a paradigm shift as cars are replacing mechanical engineering with software-driven engineering. Cars have since become mobile computing platforms with the ability to produce real-time telemetry feeds. Based on these streams, the location data, driving behaviors, component performance metrics, and usage patterns are captured in real time. The transition to software-defined architectures is opening the door to the advanced features of predictive maintenance, personalized drive experience, and over-the-air updates. The vehicles that are connected to cloud infrastructure, other vehicles, and roadside systems are connected using special wireless connections. The information that is produced in the course of regular driving is the basis of intelligent transportation systems and intelligent driver functions. Nonetheless, this technological development poses a great challenge.

The consumers are becoming more and more aware of the telemetry collection as a form of monitoring and not service provision. The information discloses very personal information concerning routine lives, places of visits, and habits. Owners of vehicles raise the question as to who the controller of this information is and how it can be misused outside its intended uses. Then comes the birth of software-defined vehicles, thereby creating a growing gap of trust between the manufacturers who want to see the detailed telemetry and the consumers who make it by simply driving the vehicle [1].

Conventional incentive systems are not effective in sealing this trust gap. The manufacturers and service platforms provide small insurance offers to promote the sharing of data. They offer promotional vouchers and open up additional features on payment of access to telemetry. These rewards seem concrete on the outside but hardly encourage a long-term engagement. The root issue does not consist in the size of the incentives but in the character of the exchange as such. Consumers view such deals as them being victims of unfair trades by giving up valuable privacy at a low cost. Even direct financial payments are uncomfortable, as they commodify personal information. Individuals do not make privacy choices by merely carrying out cost-benefit analysis. They assess exchange based on fairness schemes, expectations of reciprocity, and power. The study of behavioral economics proves that the choices made when it comes to privacy include emotional reactions and norms instead of just logical discussion. Consumers inquire whether the exchange considered their autonomy and secured their long-term interests. They are concerned with the secondary data applications, unauthorized access, and the impact that they may have in the future, which they are not able to fully predict. Unless addressed, such issues may lead to resistance as a reasonable protective measure and not technological resistance or privacy paranoia [2].

This paper suggests a radically new way of sharing telemetry incentives. Short-term compensation can be the least efficient motivator, but long-lasting and consumer-owned value will continue throughout the vehicle lifecycle. It presents the Automotive Data-Equity Loop as a full set of solutions to this predicament. The framework involves three stages that are linked together to make a value-creation cycle. Value creation will be created when ordinary vehicle operation and maintenance are performed. The process of telemetry events and records of services naturally grows as the owners drive and maintain vehicles. Value crystallization converts these raw data streams into credentials that can be verified by privacy-sensitive processing. The system transforms granular telemetry into statements concerning vehicle history without revealing delicate personal information. The realization of value is the situation where the credentials are realized by having real advantages in the resale transactions. Authenticated history lowers the buyer's uncertainty and information asymmetry in second-hand car markets. This can potentially be translated into superior pricing results, accelerated sales, and improved financing conditions. The cycle works in a vicious circle because consumers see apparent value creation and get more interested in engaging in it. The quality of participation is improved, and the completeness of the data and the credentials becomes better, which makes the whole ecosystem stronger.

The study input is a synthesis of various fields of study into a coherent model. It combines the principles of behavioral economics and the design of cryptographic architecture and user experience. The framework covers the reasons as to why individuals are resistant to sharing, how systems would transform data into verifiable claims, and what interfaces make control meaningful. It suggest that sharing of telemetry changes psychologically when done with a shift in frame of reference, such as not giving away data but creating history that has been verified. This reframing transforms the perceived exchange to the collaborative form, where consumers believe that the value is accrued to them mostly. Subsequent sections are then systematically covered in the article. Section 2 builds up the hybrid asset structure that characterizes vehicles as objects with digital strata of history. Section 3 compares incentive models based on behavioral economic analysis using experimental design proposals. Section 4 realizes consumer control by means of transparency slider interfaces that allow graduated consent. Section 5 provides governance prerequisites, risk models, and analysis techniques. Section 6 wraps up with the contribution and future research directions of applying the framework to new mobility settings.

This article makes the following contributions. First, a behavioral-economic analysis demonstrates why existing incentive models fail and why asset value enhancement is theoretically superior. Second, a three-phase framework encompassing value creation, crystallization, and realization converts telemetry into consumer-owned verifiable credentials. Third, a hybrid asset model reconceptualizes vehicles as composite assets integrating physical components with verifiable digital history layers. Fourth, a transparency slider interface operationalizes graduated consent with clear consequence mapping. Fifth, a governance

blueprint defines stakeholder roles, threat models, and institutional mechanisms for multi-party ecosystems. Sixth, a comparison with existing vehicle history services clarifies the framework's distinct value proposition. Seventh, falsifiable hypotheses and an evaluation framework enable empirical validation.

2: Related Work and Positioning

2.1: Consumer Data Incentive Models

Prior work on consumer data incentive design has explored monetary compensation, loyalty programs, and service personalization. A consistent finding demonstrates that monetary framing activates market norms that crowd out intrinsic motivations and heighten privacy concerns. Research demonstrates that privacy valuations are highly context-dependent and susceptible to framing effects, suggesting that incentive design should attend carefully to how sharing is presented, not only what is offered. The contextual integrity framework provides a theoretical basis for understanding consumer resistance. Data flows feel appropriate when they match the norms of the context in which data was generated. Telemetry generated during vehicle operation carries implicit norms about use for vehicle maintenance and safety. Repurposing it for behavioral profiling or third-party sale violates these norms and triggers resistance regardless of compensation offered [11].

2.2: Verifiable Credentials and Digital Passports

The technical foundation for the proposed framework draws on the W3C Verifiable Credentials standard, which defines a data model for cryptographically signed claims that can be verified without exposing underlying personal data. Prior applications include educational credentials, health records, and supply chain provenance. Automotive applications have been explored in the context of vehicle identity and maintenance records. However, the use of verifiable credentials as a consumer-owned resale value asset has not been previously proposed. This represents a novel application domain for verifiable credential technology [12].

2.3: Existing Vehicle History Services

A critical point of comparison involves the existing ecosystem of third-party vehicle history services, principally Carfax and AutoCheck in North America and analogous services in other markets. These services aggregate data from manufacturer reports, insurance claims, DMV records, and service center submissions to produce vehicle history reports that buyers use to assess used vehicle condition and provenance. The proposed framework differs from these services in three important respects. First, ownership structure differs fundamentally. Existing services aggregate data held by third parties and sell access to buyers. The proposed framework produces credentials owned by the vehicle owner, who controls disclosure. Second, granularity and verifiability distinguish the approaches. Existing services rely on reported events including accidents, title changes, and odometer readings at service visits and cannot verify continuous operational behavior. The proposed framework converts continuous telemetry into cryptographically verified behavioral claims. Third, incentive alignment mechanisms differ substantially. Existing services create no direct incentive for consumers to share data, as data flows to aggregators through institutional channels. The proposed framework creates a direct link between consumer sharing behavior and credential quality, aligning consumer and manufacturer interests. The framework is therefore complementary to, rather than competitive with, existing vehicle history services. Verified credentials could be incorporated into existing history report ecosystems, extending their coverage and verifiability [13].

3. The Digital Passport Architecture and Hybrid Asset Framework

3.1. Hybrid Asset Conceptual Model

Conventional ownership of vehicles considers the cars as simple physical depreciating assets after following definite depreciation curves of value that are influenced by age, mileage, and wear. Nonetheless, this model fails to consider a significant price factor other than physical condition. Asymmetry of information between the sellers and the buyers leads to the inefficiency of the market. Customers are not able to check maintenance compliance, usage, or history of incidents. Buyers do not trust honest sellers who have well-maintained vehicles and offer them unfairly low prices. Problem vehicles can be overpriced, with their sellers hiding off-putting history with incomplete paperwork. The hybrid asset model seeks to solve this lack of efficiency by redefining vehicles as compound assets with both physical components and verifiable historical layers of digital history. Electronic key identities do not stop physical degradation. The truth is that cars

cannot retain their value over time and usage no matter how well they are documented.

The digital layer of history is aimed at the extra discount caused by the information gaps instead of natural depreciation. Research of used vehicles indicates that consumers make high bids on detailed, documented repair histories. The premium is a mirror of the decreased uncertainty and not better physical condition. Credentialed credentials enhance this dynamic with more fidelity records, which cannot be tampered with or independently verified. The credentials provide detailed indications on vehicle care without revealing any sensitive personal data. Blockchain and distributed ledger technologies make it possible to have tamper-evident record keeping where various parties can have confidence without any central authority having oversight. Through these systems, the audit trails are immutable, and the modifications that do not have authorization are identified immediately by cryptographic verification mechanisms [3].

Behavioral economics gives a theoretical basis to the fact that asset value improvement is a stronger incentive than other incentive systems. Loss aversion is one of the psychological phenomena that have been extensively documented and that describe how individuals are more sensitive to possible losses than gains of the same magnitude. Sharing telemetry as a precaution against loss in the future creates better motivation than sharing the same result as receiving rewards does. In a scenario whereby the consumers perceive credential building as causing the seller to offer low prices on sales because their history cannot be verified, the exchange is non-extractive but protective. This framing of loss prevention alters the nature of the perceived transactional nature fundamentally. Consumers develop safeguarding mechanisms against financial disadvantage in the future as opposed to compensating to accept privacy risks. The system aligns the long-term consumer interests with the platform data needs. Platforms require quality telemetry in order to create plausible credentials. Credible credentials are required by consumers to safeguard the value of assets. The resulting congruency produces a win-win situation and not a zero-sum game [4].

3.2. Trust Artifact Digital Passport

The main technical realization of the hybrid asset framework is the digital passport. It converts abstract vehicle history into tangible, credentialable documents. The design of the passport must be framed with a lot of consideration in terms of consumer psychology and the perception of trust. Planning the passport as a trust artifact and not a data warehouse is critical to acceptability by consumers. The studies show that concerns about the aggregation of data are the root cause of consumers' robust resistance to sharing. Consumers have concerns regarding mass profiling, unexpected secondary purposes, and control loss. Any passport design that implies raw telemetry concentration accumulation in a central point is an invitation to ridicule, whatever the security level. The second method views the passport as a credentialing layer that has no other information besides what should be verified. Crude telemetry is highly controlled in terms of retention and access. The passport stores claims that are signed and not detailed data profiles. The content of passports is cryptographically signed claims, which are authentic claims of vehicle operation and maintenance history. Claims are created as a result of transforming raw telemetry events, service documentation, and maintenance records into statements, which are of interest to buyers. These remarks offer substantial clues without revealing personal information. The passport may have claims that it has been operating within the stress limits recommended by the manufacturer instead of having the exact location traces. Instead of storing detailed time series of driving behavior, it may validate the pattern of driving with operational profiles that are conservative as per statistical analysis. This information-focused architecture is a solution to the inherent conflict between privacy issues of consumers and buyer information requirements. Customers must be assured of the condition of vehicles and the nature of usage. The former owners must safeguard confidential information on practices, places, and personal trends. Aggregation acts to close this gap by ensuring that raw data is converted into an aggregate claim, which has enough signal and not too much exposure.

Essential to multi-stakeholder trust, tamper-evident anchoring by means of an indefeasible ledger infrastructure is the technical basis of multi-stakeholder trust. Automotive ecosystems are by their nature multifaceted in the sense that they have different parties with conflicting interests. Telemetry is created by manufacturers via car sensors. Maintenance activities are recorded by service providers. Risk is measured by the usage pattern by the insurers. Transactions are transacted in marketplaces. Credential authenticity is verified by independent verifiers. When the participants have different motivations, credibility cannot be based on the integrity of any database of a particular entity. Immutable registries create common reference points so that the unauthorized alteration of credentials can be detected by

verifying cryptographic proof. The specifics of implementation differ depending on the requirements of scalability in deployments. The principal principle of design is the same. The passport should be such that a verification can be independently made without the need to have blind faith in centralized authorities [3].

The construction of consumer mental models has a great impact on the adoption and proper utilization. The passport can work best when the consumers think about it as a closed account of proved facts they possess and have power over. This thinking model focuses more on factual proof as opposed to feelings about the quality of vehicles. It makes the owner the most dominant force to determine which information to provide and to whom. Passport is beneficial to consumers as it helps them make their vehicles worthwhile when reselling them and not as a means of monitoring the platform. Accuracy and objectivity are implied by factual verification. The owner control cues indicate an appreciation for the autonomy of the consumer. Instrumental value presents the system as consumer-empowering, as opposed to platform-extractive. Formalized levels of certification transform technical checks into commercially readable endorsements. The users (buyers) are not usually interested in verification mechanisms such as ledger architectures or digital signatures. They are interested in the meaning of credentials on the quality of the vehicle they are buying and the risk of buying it. The certifications should be aligned to understandable categories for the non-technically literate audience. Some are verified maintenance completeness, verified driving envelope, and verified component integrity. These layers are made of working currencies in which the data-equity loop is based on [4].

Ignoring that individuals often behave according to their own beliefs and values rather than the rules and instructions set by organizations, Section 3 is devoted to comparative incentive models and behavioral mechanisms.

The technical implementation of claim generation and cryptographic signing is detailed in Algorithm 2 (Section 8), which operationalizes the value crystallization phase through privacy-preserving aggregation and tamper-evident ledger anchoring.

4: Comparative Incentive Models and Behavioral Mechanisms

4.1. Three-Incentive Model Framework

The modern strategies of promoting consumer telemetry sharing fall into three main types of incentive models, producing different psychological effects. The direct payment model is an opportunity to directly pay with a direct payment in the form of a monthly payment, bonus, or micropayment. This provides conceptual transparency in which consumers are aware that the exchange is the trading of data with money. Nevertheless, explicit ways of payment, such as direct payments, often cause psychological unease by commoditizing privacy. The deal gets packaged as trading in personal data at a cost. This is distasteful to many consumers even in situations where the amount of payment seems objective. Taking payment can be experienced as a concession of the irreversible loss of privacy rather than engaging in the mutually beneficial creation of value. People tend to decline financial payment for information that is deemed privacy-sensitive despite amounts that are above what they declare they are willing to accept. This paradox indicates that decisions with regard to privacy are those of identity, autonomy, and dignity that go beyond economic calculation [5].

In access to enhanced vehicle capabilities through telemetry sharing, feature personalization models require unlocked functionality as opposed to financial payments. Customers provide data to gain access to better navigation, advanced driver-assist systems, or performance modes. This model may create positive adoption when feature utility is evidently higher than the cost of sharing. Nevertheless, feature gating can be perceived as manipulative by the consumer when he or she feels that the manufacturers purposefully held back baseline-expected functionality in order to achieve artificial leverage. The feeling of resentment increases when the gated features seem to be necessary instead of being optional. This produces pressure forces where consumers are motivated to share so that they can get access to capabilities that ought to be provided reasonably. The mental encounter becomes a matter of compulsion rather than being a matter of choice.

Asset value improvement presents a significantly different value offer. The telemetry shared by consumers is used to create a verifiable vehicle history to enhance resale market value. In contrast to the consumable incentives where money is spent and features consumed, the value of assets is built up throughout the lifecycle of the vehicle and can be realized when a vehicle is sold in a high-stakes situation. Psychological framing is changed into giving away something good to create something guarded. This reframing builds upon a number of behavioral-economic assumptions. The concept of loss aversion causes defensive interests in the future low prices to be stronger than the current bonuses. Endowment effects make people more motivated when improvements are made on assets that one already has. The long-lasting credentials are more

appealing compared to the consumable benefits, as the former favors durable benefits over the short-lasting ones [6].

4.2. Comparative Evaluation Experimental Design

Strict assessment involves experimental comparison in which psychological mechanisms are kept under controlled conditions and an outcome is measured with respect to behavior. Multi-arm research designs would have the participants exposed to varying incentive schemes, and the rates of adoption, persistence, extent of consent, perceived trust, and perceived fairness would be measured. All these variables elicit behavioral consequences and psychological processes. The hypothesis of the research suggests that asset value improvement generates greater initial adoption and extended participation than direct payment and personalizing features. Mediated effects should be fairer perceptions and fewer exploitation concerns. Asset value framing is in line with spike transactions of high stakes in the future that are of great concern to the consumers. The credibility mechanisms are crucial. The experimental applications need to have value preview screens that show realistic associations between marketplace performance and sharing decisions. Previews may also indicate the impact that verified credentials have on buyer confidence ratings or rank in search. Value previews generate the psychology of future benefits when making consent decisions in the current time [5].

The mediating factor control deserves an experimental study on its own. There are also the perceived control and the influence they may have on the relationships between incentive models and adoption patterns. Factorial structure based on an incentive model with control-level manipulations should be applied in experimental designs. High-control conditions give granular transparency sliders the ability to audit. Binary sharing decisions are realized in low-control conditions. The interaction effects are tested to establish the control mechanisms as part of successful incentive systems. Any predictions that are done numerically are placeholders until empirical measurements are taken [6].

4.3. Design Ethical Alignment

The increase in the value of assets has ethical benefits compared to the optimization of adoptions. Organizing the participation as voluntary with graded levels is an expression of respect for consumer autonomy. Depending on the user, they have the option of minimal sharing, which comes with basic credentials, or total sharing, which comes with premium credentials. This prevents the coercive nature of core vehicle functionality depending on telemetry consent. Opportunity structures maintain autonomy through an increase in choice sets. Coercive structures are undermining autonomy by limiting access to all-important services according to acceptance of surveillance.

Another principle of ethical design is data minimization by way of selective credentialing. The system must have enough data to produce verifiable, credible claims without over-maximizing the total raw data collected. Aggregate indicators and statistical summaries can enable consumers to receive valuable credentials without giving up raw telemetry traces. Safe driving credentials could be synthetically produced based on statistical analysis and not be stored as granular speed time series or location sequences. System architecture allows platform interests in believable credentials to be aligned with consumer interests in limited exposure [5].

Distributional fairness recognizes the heterogeneous consumer situations and tastes. Consumers do not value resale value equally. Others have cars that they hold over a long time and are more concerned about insurance premiums. Others are also commercially driven and appreciate maintenance cost transparency. The framework has been able to accommodate this diversity by enabling multiple value realization pathways and keeping a resale focus as the leading anchor narrative. Other value streams, such as insurance discounts and financing upgrades, can also be added as optional complements [6].

5. The Consumer Control Mechanisms and Transparency Slider Interface

The transparency slider is the main user interface tool that operationalizes the Automotive Data-Equity Loop, converting abstract consent frameworks into real user interactions. The basic design assumption is the fact that consumers decline to accept simplified binary options that presuppose all-or-nothing decisions regarding sharing telemetry. Privacy preference studies have shown that people do not have a blanket-like approval or disapproval of various types of data, their intended use, or the type of recipients to whom they should be shared. Binary consent systems do not address this complexity and encourage consumers to make awkward tradeoffs. The slider resolves this shortcoming by defining the discrete sharing levels that are matched to the particular data sets, the particular types of

certification, and anticipated trust indicators in the marketplaces. It is this mapping that allows consequences to be seen and comprehended prior to consumers committing themselves to making decisions. Users are able to view what each level entails in concrete terms as opposed to judging abstract privacy policies. The design pattern realizes graduated disclosure based on psychological studies on preference elicitation and decision architecture. When decisions are made in a way that tradeoffs become apparent, people make better decisions based on the real preferences and do not default to one extreme because of the confusion [7].

The multi-level model applies this progressive strategy by having well-spaced levels from the least to the full-fledged sharing. The low degree may include the minimum maintenance service confirmations, as some of the events are already recorded by external service providers. This produces a simple credentialed maintenance completeness with the indication of routine professional care without providing any pattern or behavioral information. Medium levels add some data types that allow stronger certifications with a disclosure of information in accordance. Telemetry analysis may provide aggregate driving envelope indicators that could support valid credentials of safe operation. These confirm that the vehicle was running on some conservative acceleration, braking, and speed limits according to statistical evidence. The system does not retain or expose granular traces once a processing of raw telemetry has been done to compute summary statistics. High-end would involve composite stress measurements and application stress indicators that would allow full certified component integrity certifications, giving a high degree of confidence to the buyer regarding the mechanical state.

Algorithm 1 (Section 8) enforces these sharing levels through programmatic data minimization, ensuring that consumers sharing at MINIMAL level expose only maintenance confirmations, while INTERMEDIATE and ADVANCED levels progressively add aggregate indicators without retaining granular traces.

All levels need to be described using plain language without using technical terminology. What is shared, what is not shared, what the credential is, and what the probable benefit in the marketplace are should be well expressed in descriptions. It can be seen in benefit-risk tradeoffs due to side-by-side comparison interfaces where privacy exposure can be seen going up with credential strength. It is this structure that makes data minimization visible and deliberate. Consumers are able to note that more certification does not necessarily imply relinquishment of full raw telemetry. They instead consist of the transfer of derived signals, aggregate statistics, and threshold-based indicators that are adequate to do credible verification. This openness is a solution to fundamental consumer issues regarding surveillance without compromising the loyalty required for credibility in the marketplace [7].

Specificity of purpose-bound certificates assists in the control mechanisms of consumer fears of repurposing data above the limits of their initial consent. It is not the initial sharing that is often the subject of privacy concerns but the concern about further spread and secondary application that is uncontrollable. The slider provides purpose specification, which enables the permission of credentials to different purposes by separate toggles or hierarchical controls to the consumer. The verification of resale, the availability of maintenance history, and the confirmation of the safety records are various purposes that have varying privacy concerns. A consumer may approve the credentials of maintenance available to be presented in the marketplace but refuse the credentials of driving behavior that may seem to be more intrusive. Purpose binding is a technical constraint and a sign of trust. "Technical restriction" refers to a system architecture that provides limits on usage of credentials by cryptographic access control and smart contract logic. Purpose specification is made with machine-enforceable constraints instead of policy commitments, which can be violated discretionally. Such a dual role modifies risk perception by limiting future system action via design as opposed to the use of institutional commitments only [8].

Audit views are also considered to give continuous transparency and accountability even when they are not used regularly. The audit interface gives consumers the ability to inspect the issued credentials, verified verification parties, contributed types of data, and also the time when the credential was generated. Although the engagement rates are low, accountability is promoted through the presence of audit views, which develops trust because of the implied accountability and the source of recourse. An audit is an option to help resolve disputes where the consumers feel that the credentials are not accurate because of recording mistakes or fist malfunctions. In case maintenance incidents were not documented appropriately, the consumers required clear channels through which they could spot the discrepancies and begin to make corrections. The process of resolution needs to be non-technical and easy to use.

Behavioral economics holds the ground in that behavioral economics is a major determinant of

privacy acquiescence regardless of the objective privacy results. Even at a constant level of objective benefits, agency perceptions raise the willingness to share. When such persons have a sense of empowerment to make meaningful decisions as opposed to being coerced into a set of demands, they become more comfortable with data sharing. The transparency slider is used as both the user experience feature and the component of the core incentive mechanisms. There can be interaction effects where there is an especially good performance of asset value enhancement in the presence of high perceived control. Transparency slider effectiveness evaluation metrics cut across a range of dimensions. Slider engagement rates are active setting adjustments to passive default acceptance. Selection levels denote distribution and demonstrate the way consumers weigh the protection of privacy and value seeking. Preference churn is used to measure the number of times that users change their preference with time [8].

6. Governance blueprint, Stakeholder Alignment, and Research Agenda

6.1. Governance Principles and Stakeholder Roles

The majority of the sociotechnical systems involving more than one organizational entity and individual consumers need strong governance that outlines accountability and safeguards consumer interests. Consumer control is the major organizing principle of the governance model foundation. The vehicle lifecycle gives individuals final control over their credentials and other sharing choices. Verification processes cannot be dependent on a wide exposure of raw telemetry to parties who may end up misusing information. This principle implements data-equity framing by making the system alter data generated by consumers into consumer-authenticated value instead of being centralized aggregation infrastructure, which mainly benefits platforms. The positions of stakeholders have to be defined perfectly with boundaries of accountability. Credential issuers (usually a car manufacturer or an authorized service provider) are confident in certain facts of vehicle history, depending on the telemetry streams or documentation of services. Credential authenticity is validated by verifiers such as marketplaces, potential buyers, financing institutions, and insurance providers by cryptographic verification of proof and ledger consultation. Checking is done without access to the underlying raw telemetry and maintains privacy and allows trust. Ledger infrastructure offers tamper-evident anchoring, which allows a third party to determine the integrity of credentials by confirming the authenticity of issuance [9].

Issuer credibility must have a clear set of requirements and continuous audits. Governance should also develop certification requirements such as technical audits of data collection systems, checks of privacy compliance, and demonstrations of security control. Regular issuer auditing maintains compliance and allows for the detection of compromised or dishonest issuers. In situations where issuers are discovered to have issued fraudulent credentials, governance should identify repercussions such as the possibility of revoking certification and systematic re-examination of the credentials that have been issued in the past. The avenues of revocation and correction are very crucial towards ensuring credibility in the long term. False or fake credentials should be cancelable without inclusion of adverse lifetime records against the victims of fraud. The process of correction should be transparent to the consumer and should not involve the use of complicated technical navigation. The reason that revocation mechanisms are important is that credential trustworthiness is the basis of resale markets [9].

The algorithmic implementation of these stakeholder roles is detailed in Algorithms 2-4 (Section 8), which demonstrate how issuers generate credentials, verifiers validate authenticity, and ledger infrastructure provides tamper-evident anchoring without centralizing control.

6.2. Threat Model and Mitigation

Realistic threat modeling recognizes participants in an ecosystem as having incentives that may encourage gaming or adversarial behavior. Consumers could seek to manipulate the process of credential generation in order to get maximum resale value by driving temporarily during the data collection. The service providers may be inclined to overestimate the level of maintenance to satisfy the clients who seek high qualifications. Marketplaces may compel consumers to opt to share as much as possible to enhance buyer confidence and speed of transacting. Outside intruders may seek to commit fraud on credentials or execute privacy attacks based on re-identification of claims by alleged anonymity.

The mitigation of consumer gaming needs to be monitored continuously, and anomalies in the statistics need to be found instead of being approached as acts of spot checks at the expected times. There should be systems whereby continuous sampling is used, and temporary modification of behavior would not work. Substantial verification

of suspicious patterns is activated by statistical analysis. Attestation of service providers creates an independent confirmation that increases the credibility of maintenance claims. The mitigation process of service provider fraud would involve periodic auditing of service records that may involve random verification by using manufacturer warranty systems. The market pressure demands a policy of governance that has forbidden the facilitation of conditioning transactions on the definite levels of sharing. The attack of forgery requires the strong cryptographic design of credentials based on the digital signatures and the ledger anchoring with tamper-evidence. Attacks on privacy that seek re-identification must have a granularity of claims that allow adequate signals to be used by buyers that still permit reconstruction of the individual usage patterns but not accurately [10].

Aggregation inference attacks represent an additional threat vector. Even aggregate credentials may enable re-identification or sensitive inference when combined with external data sources. Adversaries might correlate credential patterns with publicly available information to re-identify vehicle owners or infer sensitive behavioral characteristics. Mitigations include differential privacy techniques in aggregation processes, minimum data volume requirements before credentials are issued preventing inference from small samples, and regular privacy audits of credential content against known re-identification techniques. These protections ensure that privacy preservation remains robust even as external data sources proliferate [10].

Manufacturer data monopoly concerns arise because manufacturers may resist the framework as it transfers data value to consumers, potentially threatening existing data monetization models. This represents both a technical threat and an adoption challenge. The framework must demonstrate that manufacturer participation generates sufficient indirect benefits including increased telemetry adoption rates, improved product data quality, customer loyalty, and regulatory goodwill to offset the loss of exclusive data control. Without manufacturer participation, the framework cannot achieve the scale necessary for meaningful market impact [15].

6.3: Framework Limitations

6.3.1: Falsifiable Hypotheses

The framework generates five specific, quantified, testable hypotheses requiring empirical validation.

Hypothesis 1 (Adoption Superiority): In a controlled experiment with random assignment to incentive conditions, asset value enhancement will generate adoption rates at least twenty percentage points higher than direct payment and feature personalization conditions at six-month follow-up.

Hypothesis 2 (Persistence Superiority): Participants in the asset value enhancement condition will maintain sharing at their initial consent level for significantly longer duration than participants in alternative conditions, with hazard ratio below 0.7 for consent withdrawal.

Hypothesis 3 (Fairness Mediation): The adoption advantage of asset value enhancement over direct payment will be statistically mediated by perceived fairness scores, with the indirect effect accounting for at least 40% of the total effect.

Hypothesis 4 (Market Premium): In observational market studies with econometric controls for vehicle age, condition, and make or model, vehicles with advanced-level credential portfolios will command sale price premiums of at least 3% compared to equivalent vehicles without credentials.

Hypothesis 5 (Slider Engagement): Consumers presented with the transparency slider interface will select intermediate or advanced sharing levels at higher rates than consumers presented with binary consent, and will exhibit lower rates of consent withdrawal at twelve-month follow-up [10].

6.3.2 Evaluation Blueprint and Research Questions

The blueprint of evaluation provides a coordinated research agenda to empirically prove the automotive data-equity loop framework. This agenda is divided into three major research questions. Research Question 1 will answer the question of whether the increase in asset value positively affects willingness to share telemetry over direct payment and feature personalization models. This necessitates an experimental comparison under controlled exposure, in which participants are subjected to various incentive conditions, and adoption, persistence, and deepening of consent are measured. Research Question 2 will look at the effect of the transparency slider control on its adoption and persistence regardless of incentive level. This involves experimental manipulation of control systems in constant levels of benefits. Research Question 3 explores the possibility of verified credentials having a measurable impact on the resale market results, such as the sale price, the duration of the listing process, and the buyer confidence indicators. This would involve observational market research of vehicles with different levels of credentials, with other things held constant.

The proposed methodology runs both the controlled laboratory studies and the observational studies in the real world. The user studies would involve recruiting participants, presenting them to various incentive accounts and slider designs, and comparing the preferences stated and the real opt-in decisions. Market analysis will demand collaboration with used-car dealers or manufacturers to retrieve transaction information. Approximation of causality in observational designs is a problem as credentialed vehicles can differ on nonmeasured dimensions systematically compared to noncredentialed vehicles. More complex econometric methods are required to separate credential effects and selection effects [10].

Open research directions do not limit themselves to the short-term evaluation priorities. The differences in cross-cultural preferences for privacy may have a significant influence on the adoption patterns that need international comparative research. The long-run impacts on the ecosystem should also be studied as more people adopt the credential. Combinations with new mobility patterns such as vehicle subscription applications and self-driving fleets, might necessitate modifications in the framework because the old systems of ownership might not be relevant.

6.4: Limitations and Future Work

The existing framework construction revolves more around the resale contexts that imply the hypothesis that resale value is the most widely persuasive consumer motive. Nevertheless, there is logic behind this to other value-realization contexts. The fact that a reduction in the insurance premiums is made with the use of validated safe driving qualifications serves to generate immediate value. The improved terms of financing could be achieved when the lenders check maintenance histories. The use of checking credentials can be beneficial in fleet management applications to optimize the vehicle allocation and maintenance scheduling. Both apps have to adjust the general framework principles while adhering to the basic premise of transforming consumer-generated data into consumer-owned value.

Scalability is also a consideration that should be given attention, whereby systems that were initially deployed as prototype demonstrations evolve into ecosystem-wide deployments. Technical scalability is the ability to generate credentials and store, verify, and anchor ledgers with unlimited streams of telemetry without reducing the performance of the system. Scalability of governance involves the creation of sustainable institutional frameworks to issue certifications, resolve disputes, and conduct continuous audits. Market scalability is based on the attainment of critical mass of adoption where credentials develop value where buyers acknowledge them and trust credentials. Standardization activities within the manufacturers and service providers are also basic future tasks. The credential format and verification protocols used by proprietors of credentials make ecosystems less portable and valuable. Standardization should be balanced between consistency, which allows wide recognition, and flexibility, which allows manufacturers to differentiate and innovate [9].

7: Adoption Challenges and Limitations

7.1: The Critical Mass Problem

The most significant adoption challenge involves the critical mass problem. Verified credentials generate resale value only if buyers recognize and value them, but buyers will only recognize credentials if they are widely adopted. This chicken-and-egg dynamic represents a common barrier to two-sided market adoption. Several strategies can address this challenge. Manufacturer-led seeding enables manufacturers to issue credentials for all vehicles in their fleet regardless of consumer opt-in, establishing a baseline of credential availability that buyers can rely upon. Marketplace integration through early integration with major used-vehicle marketplaces creates buyer-facing visibility that drives consumer awareness. Insurance and financing partnerships create credential-based premium and rate adjustments providing immediate, tangible value that does not depend on resale market adoption. Regulatory support through disclosure requirements for credential availability in vehicle listings could accelerate marketplace adoption [14].

7.2: Manufacturer Incentive Alignment

Manufacturers currently benefit from exclusive control over vehicle telemetry data. The proposed framework transfers credential ownership to consumers, potentially threatening existing data monetization models. Manufacturer participation requires demonstrating that the indirect benefits of the framework including higher telemetry adoption rates, improved data quality, customer loyalty, and regulatory goodwill outweigh the costs of reduced data exclusivity. This represents an empirical question requiring market studies of manufacturer data economics. The framework must demonstrate that manufacturer participation generates sufficient

indirect benefits to offset the loss of exclusive data control [15].

7.3: Framework Limitations

Several limitations require acknowledgment. The theoretical nature of performance claims means all performance assertions represent hypotheses rather than measured outcomes. The evaluation framework defines the empirical work required to validate or refute these claims. Until this work is completed, the framework represents a research proposal rather than a validated solution. Resale context bias reflects that the framework is primarily oriented toward resale value as the primary consumer motive. It may not apply equally to consumers who hold vehicles long-term, lease, or use subscription models. Alternative value streams including insurance premium reduction and financing term improvement are mentioned but not deeply analyzed. Cross-cultural applicability concerns arise because privacy preferences, loss aversion magnitudes, and fairness norms vary significantly across cultures. The behavioral-economic predictions underlying the framework may not generalize across international markets without modification. Technical scalability at an ecosystem-wide scale potentially involving hundreds of millions of vehicles raises engineering challenges not addressed in detail. Ledger architecture choices including permissioned versus permissionless systems and on-chain versus off-chain storage have significant implications for scalability, cost, and governance, requiring dedicated technical analysis [15].

8: Algorithmic Implementation Framework

This section provides pseudocode algorithms operationalizing the Automotive Data-Equity Loop's core technical mechanisms. The algorithms demonstrate how privacy-preserving aggregation, cryptographic credential issuance, and multi-factor verification can be implemented while maintaining the graduated consent model described in Section 5. Algorithm 1 enforces data minimization at the collection layer by transforming raw telemetry into consent-level-appropriate aggregate claims. Algorithm 2 operationalizes value crystallization through cryptographic signing and tamper-evident ledger anchoring. Algorithm 3 enables independent verification at the point of value realization without requiring verifiers to access underlying raw telemetry. Algorithm 4 orchestrates the complete three-phase workflow, demonstrating how the framework operates from initial data collection through resale transaction verification.

ALGORITHM 1: Privacy-Preserving Telemetry Aggregation

Input: RawTelemetry R = {odometer, engine_hours, hard_braking, maintenance, avg_speed, battery_soc}
ConsentProfile P = {vehicle_id, owner_id, level ∈ {MINIMAL, INTERMEDIATE, ADVANCED}}
Output: AggregatedClaims A (no granular traces)

```
A ← ∅

IF P.level ≥ MINIMAL THEN
  A ← A ∪ {maintenance_complete: (R.maintenance ≠ ∅),
       maintenance_items: R.maintenance}

IF P.level ≥ INTERMEDIATE THEN
  A ← A ∪ {avg_speed_band: LOW if v < 60 | MEDIUM if v < 100 | HIGH,
       hard_braking_band: LOW if b < 5 | MEDIUM if b < 20 | HIGH}

IF P.level ≥ ADVANCED THEN
  A ← A ∪ {odometer_km, engine_hours}
  IF R.battery_soc exists THEN
    A ← A ∪ {battery_soc_pct}

RETURN A
```

Consent level to credential mapping:

- MINIMAL → "Verified Maintenance Completeness" (Privacy exposure: Low)
- INTERMEDIATE → "Verified Safe Operation" (Privacy exposure: Medium)
- ADVANCED → "Verified Component Integrity" (Privacy exposure: Higher)

ALGORITHM 2: Digital Passport Issuance (Value Crystallization)

Input: RawTelemetry R, ConsentProfile P, Issuer I = {id, private_key}
Output: DigitalPassport D = {claims, signature, ledger_anchor}

```
A ← Aggregate(R, P)                                  // Algorithm 1
type ← CONSENT_MAP[P.level].credential_type

D ← {credential_id: UUID(),
     vehicle_id: R.vehicle_id,
     owner_id: P.owner_id,
     issuer_id: I.id,
     credential_type: type,
     claims: A,
     issued_at: now(),
     consent_level: P.level}
```

D.signature ← Sign(I.private_key, CanonicalJSON(D))
D.ledger_anchor ← Ledger.Anchor(SHA256(CanonicalJSON(D)))

RETURN D

Note: Signing payload excludes signature and ledger_anchor fields to prevent circular reference. Production implementations should replace SHA256-HMAC with ECDSA asymmetric signature algorithms.

ALGORITHM 3: Credential Verification (Value Realization)

Input: DigitalPassport D,
Verifier V = {trusted_issuers, ledger},
Issuer I (public key only)
Output: VerificationResult = {issuer_trusted, sig_valid,
ledger_valid, overall_valid}

issuer_trusted ← (D.issuer_id ∈ V.trusted_issuers)
sig_valid ← Verify(I.public_key, CanonicalJSON(D), D.signature)
ledger_record ← V.ledger.Lookup(D.ledger_anchor)
ledger_valid ← (ledger_record ≠ null)
AND (ledger_record.hash = SHA256(CanonicalJSON(D)))
overall_valid ← issuer_trusted AND sig_valid AND ledger_valid

RETURN {issuer_trusted, sig_valid, ledger_valid, overall_valid}

ALGORITHM 4: Data-Equity Loop Orchestration

Input: RawTelemetry R, ConsentProfile P, Issuer I, Verifier V
Output: VerificationResult (at point of resale)

// Phase 1: Value Creation
1. Collect R on-device during normal vehicle operation
// No data leaves the vehicle at this stage

// Phase 2: Value Crystallization
2. D ← IssueCredential(R, P, I) // Algorithm 2
// Raw telemetry replaced by privacy-preserving signed claims

// Phase 3: Value Realization
3. result ← Verify(D, V, I) // Algorithm 3
// Buyer/marketplace validates credential at point of resale

4. RETURN result

Governance Roles:

Credential Issuers - Automotive manufacturers or certified service providers holding private keys for credential signing. Issuers must pass certification requirements including technical audits, privacy compliance verification, and security control demonstration before credentials are accepted by verifiers.

Credential Verifiers - Marketplaces, prospective buyers, financing institutions, or insurance providers holding issuer public keys. Verifiers validate credentials without accessing raw telemetry and maintain trusted issuer registries.

Ledger Infrastructure - Tamper-evident registry implemented through permissioned blockchain systems such as Hyperledger Fabric or RFC-3161 compliant timestamp authorities. The ledger stores credential hashes providing immutable reference points and enabling post-sale revocation checks.

Transparency Slider Graduated Consent Interface:

Consumers select sharing levels through the interface described in Section 5. The system enforces data minimization at Algorithm 1, ensuring that only consent-level-appropriate aggregations are computed and stored.

Production Hardening Requirements:

- **Cryptographic Signing:** ECDSA or similar asymmetric signature algorithms where verifiers require only public keys for validation
- **Ledger Architecture:** Permissioned blockchain such as Hyperledger Fabric or RFC-3161 compliant timestamp authorities for tamper-evident anchoring
- **Revocation Registry:** Credential revocation lists or status registries enabling verifiers to check credential validity before acceptance
- **Key Recovery Protocol:** Consumer wallet recovery mechanisms for credential access restoration in case of device loss or failure
- **Privacy Audit:** Regular validation ensuring credential metadata patterns cannot enable re-identification of granular driving behavior through timing correlation or pattern matching [16]

The algorithms implement the three-phase framework architecture described in Section 3. Algorithm 1 enforces data minimization by design, preventing raw trace exposure while maintaining sufficient signal fidelity for buyer-relevant claims. Algorithm 2 operationalizes value crystallization through cryptographic signing and ledger anchoring, producing tamper-resistant credentials owned by consumers. Algorithm 3 enables independent verification at the point of value

realization, allowing buyers and marketplaces to validate credential authenticity without accessing underlying personal data. This algorithmic implementation demonstrates that the Automotive Data-Equity Loop framework is not merely conceptual but represents a technically feasible approach to aligning telemetry sharing incentives with consumer autonomy and long-term value creation.

Table 1: *Comparative Analysis of Telemetry Sharing Incentive Models. [5, 6]*

Incentive Model	Primary Mechanism	Psychological Response	Key Limitation
Direct Payment	Monetary compensation through monthly payments or bonuses	Commodifies privacy; feels like selling personal information	Creates discomfort by framing exchange as permanent privacy loss rather than mutual value creation
Feature Personalization	Access to enhanced vehicle capabilities conditional on data sharing	May generate resentment when features appear artificially withheld	Risks manipulation perceptions and coercive dynamics when consumers feel forced to share for baseline functionality
Asset Value Enhancement	Building verifiable credentials that increase resale market value	Protective rather than extractive; leverages loss aversion and endowment effects	Requires credibility mechanisms demonstrating plausible links between sharing and future resale outcomes

Table 2: *Transparency Slider Sharing Levels and Corresponding Certifications. [8]*

Sharing Level	Data Categories Shared	Credential Type Generated	Privacy Exposure
Minimal	Maintenance service confirmations only	Verified Maintenance Completeness	Low - service records already exist independently; no behavioral data revealed
Intermediate	Maintenance records plus aggregate driving envelope indicators	Verified Safe Operation	Medium—statistical summaries of driving patterns without granular traces or location data
Advanced	Maintenance, driving indicators, component stress monitoring, usage intensity metrics	Verified Component Integrity	Higher, more comprehensive history providing maximum buyer confidence while using derived signals

Table 3: *Stakeholder Roles and Responsibilities in the Data-Equity Ecosystem. [9]*

Stakeholder	Primary Responsibility	Trust Mechanism	Accountability Requirement
Credential Issuers	Attest to vehicle history facts based on telemetry and service documentation	Technical capability for accurate claim generation; institutional trustworthiness resisting fraud	Must pass certification requirements including technical audits, privacy compliance verification, and security control demonstration
Verifiers	Validate credential authenticity through cryptographic proof verification and ledger consultation	Independent verification without accessing raw telemetry	Must follow governance policies restricting secondary use and preventing coercive marketplace pressure
Ledger Infrastructure	Provide tamper-evident anchoring enabling detection of unauthorized modifications	Immutable reference point trusted by multiple parties without centralized control	Must maintain cryptographic integrity and enable independent verification across the ecosystem.

Table 4: *Research Questions and Proposed Evaluation Methodologies. [10]*

Research Question	Methodology	Key Metrics	Expected Outcome

RQ1: Does asset value enhancement increase willingness to share versus payments/personalization?	Controlled experimental comparison with multi-arm design	Adoption rates, persistence duration, depth of consent, perceived fairness	Asset value framing produces higher adoption and retention mediated by fairness perceptions [TBD]
RQ2: Does transparency slider control increase adoption and persistence?	Factorial experimental design crossing incentive models with control levels	Slider engagement rates, distribution of sharing levels, preference churn over time	High-control conditions amplify incentive effectiveness through interaction effects [TBD]
RQ3: Do verified credentials affect resale market outcomes?	Observational market studies with econometric controls for confounding factors	Sale price premiums, listing duration, buyer inquiry rates, and financing terms	Credentials reduce uncertainty-driven price discounts in used vehicle markets [TBD]

Table 5: *Quantitative Metrics for Framework Evaluation. [10], [14]*

Metric	Definition	Target
Adoption Rate	Fraction activating sharing	>40% at 6 months
Persistence Rate	Fraction maintaining consent at 12 months	>70%
Consent Depth	Distribution of sharing levels	>50% at Level 2+
Perceived Fairness	Survey scale (1–7)	Mean >5.0
Price Premium	Sale price differential	>3%
Listing Duration	Days to sale reduction	>10% reduction
Credential Verification Rate	Fraction of buyers verifying	>60%

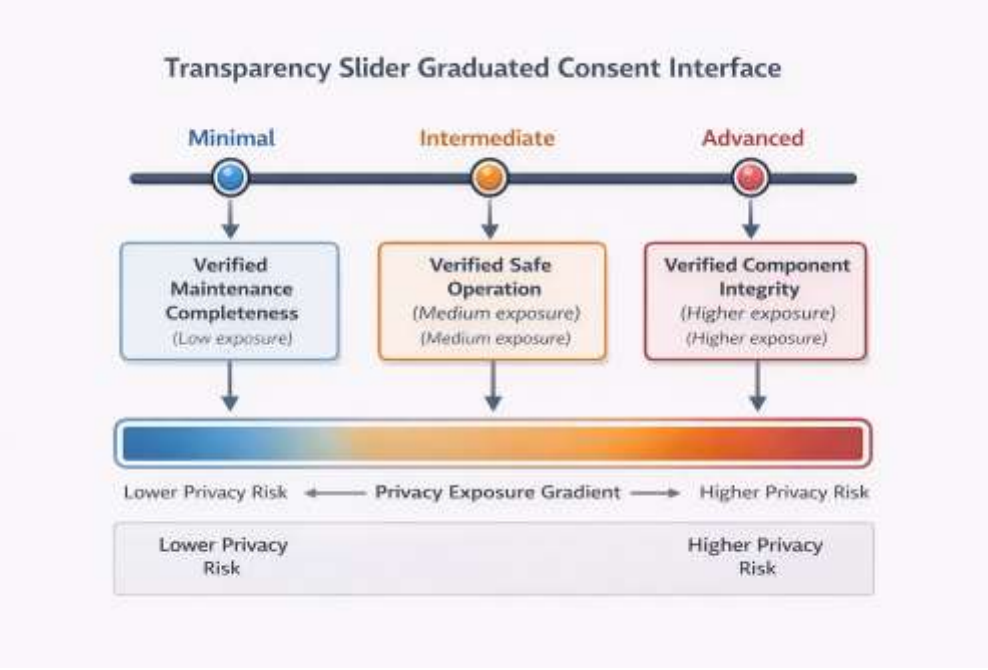

Figure 1: *Transparency Slider Graduated Consent Interface. Consumers select sharing levels through the interface, with the system enforcing data minimization at Algorithm 1.*

9. Conclusions

This article has developed the Automotive Data-Equity Loop as a socio-technical innovation addressing the fundamental trust gap in software-defined vehicle telemetry sharing. The framework's central insight demonstrates that durable, consumer-owned value accumulated through

verified credentials proves more effective than short-term compensation or consumable benefits. By converting raw telemetry into tamper-resistant, cryptographically verifiable credentials that reduce buyer uncertainty, the framework transforms data sharing from extraction to empowerment. This reframing addresses core behavioral-economic drivers of consumer resistance rather than attempting to overcome objections through larger incentives or persuasive messaging.

The contributions span four primary domains. First, the hybrid asset framework reconceptualizes vehicles as composite assets integrating physical components with verifiable digital history layers. This targets uncertainty-driven depreciation while providing consumers an intuitive model for understanding how sharing protects financial interests. Second, the comparative incentive model establishes behavioral-economic rationale for why asset value enhancement outperforms direct payment and feature personalization through loss aversion, endowment effects, and fairness perceptions. Third, the transparency slider operationalizes meaningful control through multi-level interfaces mapping sharing choices to certification outcomes. Fourth, the governance blueprint establishes stakeholder roles, threat models, and institutional mechanisms for maintaining system credibility across multi-party ecosystems.

Practical implications extend to multiple constituencies. Automotive manufacturers can deploy this framework as an alternative to approaches generating consumer resistance. Rather than offering small discounts or gating features manipulatively, manufacturers position telemetry sharing as building consumer-owned assets and protecting resale value. Marketplace platforms can integrate verified credentials into listing interfaces and search algorithms, providing buyers higher-confidence signals about vehicle condition. This potentially increases transaction velocity and reduces negotiation friction. Policymakers can recognize the framework as demonstrating how data ecosystems align with consumer benefit through transparency and control rather than requiring restrictive regulation.

However, realizing these implications requires rigorous empirical validation. Key questions remain about whether asset value enhancement increases adoption relative to alternatives, whether transparency controls amplify effects, and whether credentials affect actual resale outcomes. Controlled experiments comparing incentive models will test predictions about fairness perceptions and control as moderating factors. Observational market studies employing causal inference methodologies will assess whether credentials affect transaction outcomes, including prices, listing durations, and buyer inquiry rates.

The Automotive Data-Equity Loop instantiates a broader principle applicable beyond automotive contexts. Consumer-generated data creates sustainable value when systems ensure value accrues primarily to consumers themselves. As physical assets become increasingly software-defined and data-generating, aligning data practices with consumer autonomy intensifies across domains. The framework offers a template treating consumers as asset owners deserving equitable value distribution rather than data sources for platform extraction. Privacy becomes a design constraint producing better outcomes rather than an obstacle to overcome.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] Juan Contreras-Castillo et al., "Internet of Vehicles: Architecture, Protocols, and Security," IEEE Xplore, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7892008

[2] Alessandro Acquisti et al., "Privacy and human behavior in the age of information," Science, 2015. [Online]. Available: https://www.science.org/doi/10.1126/science.aaa1465

[3] Konstantinos Christidis, Michael Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, 2016. [Online].

Available: https://ieeexplore.ieee.org/document/7467408

[4] Daniel Kahneman, Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," The Econometric Society, 1979. [Online]. Available: https://www.jstor.org/stable/1914185

[5] Alessandro Acquisti et al., "The Economics of Privacy," Journal of Economic Literature, 2016. [Online]. Available: https://www.aeaweb.org/articles?id=10.1257/jel.54.2.442

[6] Richard H. Thaler, Cass R. Sunstein. "Libertarian paternalism," American Economic Review, 2003. [Online]. Available: https://www.aeaweb.org/articles?id=10.1257/000282803321947001

[7] Helen Nissenbaum, "Privacy as Contextual Integrity," Washington Law Review, 2004. [Online]. Available: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

[8] Noah Apthorpe et al., "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic," arXiv:1705.06805 [cs.CR], 2017. [Online]. Available: https://arxiv.org/abs/1705.06805

[9] Ali Dorri et al., "Blockchain for IoT security and privacy: The case study of a smart home," IEEE Xplore, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7917634

[10] Cynthia Dwork, Aaron Roth, "The Algorithmic Foundations of Differential Privacy," Emerald Insight, 2014. [Online]. Available: https://www.emerald.com/fttcs/article-abstract/9/3-4/211/1332491/The-Algorithmic-Foundations-of-Differential?redirectedFrom=fulltext

[11] Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review*, 2004. [Online]. Available: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

[12] W3C Recommendation, "Verifiable Credentials Data Model v2.0" 2025. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[13] Feng Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," IEEE Xplore, 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7538424

[14] Giulio Zanella, "Discrete Choice with Social Interactions and Endogenous Memberships," Journal of the European Economic Association, 2007. [Online]. Available: https://www.jstor.org/stable/40005163

[15] Gary S. Becker, Casey B. Mulligan, "The Endogenous Determination of Time Preference," The Quarterly Journal of Economics, 1997. [Online]. Available: https://www.jstor.org/stable/2951254

[16] C. Adams et al., "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)," RFC 3161, 2001. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3161