Building a Trusted Framework for Responsible Telematics Data Access

Executive Summary

Connected vehicles generate increasing volumes of telematics data that can improve understanding of vehicle performance, driver behavior, roadway conditions, and crash causation. These data offer significant opportunities to advance roadway safety by enabling more comprehensive evaluation of advanced driver assistance systems (ADAS), automated driving technologies, vehicle safety features, and transportation infrastructure than is possible through traditional crash reports or aggregated datasets alone.

At the same time, vehicle-specific telematics data may include proprietary vehicle information as well as sensitive information about drivers and passengers. As connected vehicle technologies continue to evolve, policymakers, automakers, researchers, and consumers share an interest in ensuring that telematics data can support legitimate safety research without compromising privacy, cybersecurity, intellectual property, or public trust.

This paper proposes a set of design considerations and key elements for establishing a framework for enabling responsible access to vehicle-specific telematics data for independent safety research. If established through future legislation, standards development, and public-private collaboration, such a framework could complement existing vehicle safety, privacy, and cybersecurity requirements by outlining governance structures, technical safeguards, and implementation considerations that support meaningful safety research while limiting access to what is necessary for approved research purposes.

Rather than creating an entirely new regulatory structure, the paper presents an approach that builds upon existing institutional responsibilities, established privacy principles, and current transportation safety programs. The concepts presented here are intended to inform future legislation, standards development, pilot programs, and broader implementation efforts involving government, industry, academia, and other qualified research organizations.

MITRE

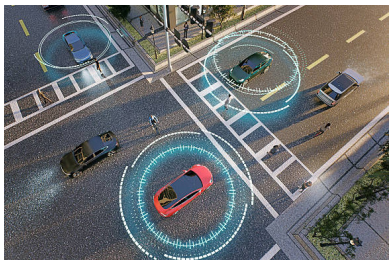
Research Objectives and Use Cases

Many important transportation safety questions cannot be adequately answered using currently collected data, aggregated data, or de-identified datasets. Understanding how individual vehicles perform under specific operating conditions, how safety systems respond during safety-critical events, and how vehicles interact with the roadway environment over time often requires collection of and access to vehicle-specific telematics data.

Providing qualified researchers with responsible access to these data would benefit a broad range of stakeholders, including vehicle manufacturers, transportation agencies, regulators, and ultimately the traveling public. The concepts presented in this paper are intended to support research that improves understanding of vehicle technologies, roadway infrastructure, and transportation safety initiatives beyond what existing data sources can provide. At the same time, they are designed to protect individual privacy, proprietary information, and public trust.

Vehicle Technology Evaluation

Vehicle-specific telematics data can improve understanding of how advanced vehicle technologies perform under real-world conditions, providing evidence to support future vehicle design, software development, safety system performance, and evidence-based transportation safety policy. Representative research applications include:



- Evaluating the effectiveness of ADAS across different roadway, weather, and traffic conditions.
- Measuring the real-world, exposure-adjusted effectiveness of vehicle safety technologies and infrastructure design countermeasures.
- Comparing automated driving system performance with human drivers operating in similar environments.
- Understanding software performance across versions and vehicle configurations.
- Identifying factors contributing to crash causation and crash severity.

Roadway Infrastructure and Operations

Vehicle-specific telematics data also provides an opportunity to evaluate transportation infrastructure in ways that are difficult using traditional crash databases alone. By fusing telematics data with known infrastructure (e.g., road curvature), researchers may examine how roadway geometry, traffic control devices, work zones, speed management strategies, and other infrastructure improvements influence safety outcomes. These analyses can help transportation agencies identify which infrastructure investments produce measurable reductions in crashes, injuries, and safety-critical events while supporting more effective allocation of public resources.

Transportation Safety Policy

Beyond vehicle and infrastructure research, vehicle-specific telematics data can support evaluation of broader transportation safety initiatives, including educational campaigns, infrastructure investments, and emerging mobility technologies. Because telematics data provides continuous operational information rather than isolated crash observations, it offers opportunities to assess safety interventions before their effects become visible in traditional crash statistics.

Framework Requirements and Design Challenges

Developing a future telematics research framework requires balancing several objectives, some of which may conflict with each other. Improving access to safety-relevant data alone is insufficient. Any framework established to support vehicle-specific telematics research must also maintain consumer trust, protect proprietary information, support high-quality research, and operate within an evolving legal and regulatory environment. The considerations below represent key design challenges that any future framework would need to address.

Privacy and Consumer Trust

Consumers increasingly expect transparency regarding how their vehicle-specific telematics data is collected, shared, and used. Vehicle-specific telematics data may reveal detailed information about travel patterns, driving behavior, vehicle usage, and other aspects of daily life. Recent regulatory attention to connected-vehicle data practices has reinforced the importance of limiting secondary uses of telematics data and ensuring that research activities remain clearly separated from commercial data monetization, targeted advertising, insurance pricing, and other unrelated uses. Maintaining public trust therefore requires both privacy protections that are proportional to the sensitivity of the data being used and appropriate oversight throughout the research process.

Protection of Proprietary Information

Telematics data may also contain commercially sensitive information about vehicle performance, software behavior, calibration strategies, and other proprietary technologies. Manufacturers have a need to protect their intellectual property while still contributing to independent safety research. Accordingly, any future framework would need to provide mechanisms that enable meaningful research without requiring unrestricted disclosure of proprietary information. Secure research environments, controlled analytical access, publication review procedures, and appropriate legal protections represent examples of measures that could help balance these objectives.

Research Quality and Interoperability

Meaningful safety research depends not only on access to data but also on the quality and consistency of the information being analyzed. Differences in data definitions, event triggers, sampling methodologies, software metadata, and reporting practices can make it difficult to compare findings across manufacturers or combine datasets for broader analysis. Improving interoperability therefore requires more than expanding access. It also requires common technical standards, consistent reporting practices, and shared data definitions that support reliable, reproducible, and scientifically defensible research outcomes.

Legal and Governance Considerations

Vehicle-specific telematics data exists within a complex legal environment that includes motor vehicle safety requirements, consumer protection law, privacy statutes, cybersecurity obligations, breach notification requirements, and, in some cases, international data protection regimes. Questions surrounding telematics data are often less about ownership than about who may access, use, disclose, retain, or transfer information under specific circumstances.

Rather than creating entirely new governance structures, a future framework could build upon existing institutional authorities while establishing clear, consistent rules for research access.

A future framework designed around these principles could provide confidence to consumers, manufacturers, researchers, and policymakers that vehicle-specific telematics data is being used only for legitimate safety purposes under appropriate technical, legal, and administrative safeguards.

Framework Architecture

Meeting the objectives described in the previous section requires an approach that aligns data collection and access with research needs while preserving appropriate privacy and governance protections. One possible approach to implementing a national telematics research framework would be to organize research access through a layered architecture that aligns the level of data access with the sensitivity of the data and the needs of the approved research. The objective would be to provide researchers with sufficient information to answer safety questions while minimizing unnecessary access to personally identifiable information or proprietary vehicle data. In practice, most safety research can be conducted using de-identified or pseudonymous data, with access to more sensitive information reserved for a limited set of approved use cases. Under this approach, the architecture could include three research access tiers, with progressively stronger governance and technical safeguards as data sensitivity increases.

Tier 1: Aggregate and De-identified Data

The first tier could support research that can be conducted using aggregate statistics or fully de-identified datasets. These data would enable broad analyses of crash trends, vehicle performance, roadway conditions, and other transportation safety topics without exposing individual vehicles or drivers. Because the privacy risk is comparatively low, this tier could provide the broadest research access while requiring the fewest administrative controls.

Tier 2: Pseudonymous Vehicle-Level Data

The second tier could provide approved researchers access to pseudonymous vehicle-level records within a secure research environment. Vehicle identifiers would be replaced with privacy-preserving linkage methods that allow researchers to associate multiple events with the same vehicle over time without revealing its identity.

This tier would likely support most of the approved safety research because it enables longitudinal analyses, evaluation of safety system performance, and investigation of safety-critical events while substantially reducing privacy risks associated with direct identifiers.

Tier 3: Restricted VIN Linkage

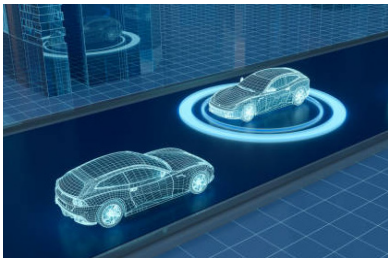
The highest tier could provide access to direct vehicle identifiers only when necessary to support approved safety objectives. Examples include linking telematics events to crash reports, production configurations, recall information, or other vehicle datasets that cannot reasonably be connected through pseudonymous identifiers alone.

Requests for Tier 3 access could require additional justification and independent review. Access could be limited to the minimum information necessary to complete the approved research objective and could be subject to enhanced governance, auditing, and security controls.

Governance Considerations

The effectiveness of a future telematics research framework depends not only on technical safeguards but also on governance mechanisms that establish clear accountability, consistent decision making, and public confidence. Regardless of the specific implementation model adopted, a future framework would likely require governance mechanisms that define who may access vehicle-specific data, how requests are evaluated, and how approved research activities are monitored over time. Together, these governance considerations illustrate one possible approach to ensuring that vehicle-specific data is accessed only when appropriate, used only for approved purposes, and protected throughout the research lifecycle.

Research Eligibility



One element of a future governance framework could be the establishment of common eligibility criteria for organizations seeking access to vehicle-specific telematics data. Research proposals could be limited to clearly defined transportation safety objectives, including evaluation of vehicle technologies, roadway infrastructure, crash causation, safety countermeasures, and related public-interest research.

Access could be limited to qualified organizations capable of conducting independent transportation safety research. Eligible organizations may include accredited universities, nonprofit safety research institutes, federally funded research and development centers, and other entities that demonstrate appropriate technical expertise, institutional safeguards, and conflict-of-interest management. Organizations participating in the framework would remain responsible for complying with applicable legal, regulatory, and institutional requirements governing research, including Institutional Review Board oversight where required.

Project Review

A second governance element could be an independent review process for evaluating requests for vehicle-specific telematics data. Once eligibility has been established, requests for vehicle-specific data could undergo an independent review process before access is granted. The review would evaluate:

- the proposed safety objective;
- the necessity of the requested data;
- whether a less sensitive dataset could satisfy the research objective;
- privacy and cybersecurity risks;
- researcher qualifications, institutional safeguards, and compliance with applicable legal, regulatory, or institutional review requirements; and
- plans for publication and dissemination of findings.

This review process would provide a consistent method for balancing research value against potential privacy, commercial, and security risks. It would be intended to complement, rather than replace, existing legal, regulatory, and institutional oversight mechanisms.

Data Use Agreements

Following project approval, participating organizations could operate under standardized data use agreements that establish common conditions for access and data stewardship. These agreements would establish purpose limitations, prohibit unauthorized re-identification and onward transfer, define data retention requirements, require secure storage, and establish incident reporting and audit obligations.

Together, these governance mechanisms would ensure that researchers receive access to the information necessary to conduct meaningful safety research while maintaining accountability for the responsible stewardship of sensitive data.

Privacy, Security, and Data Management

Privacy and security protections are foundational elements of any future research access framework rather than independent compliance activities. Any framework established to support vehicle-specific telematics research would likely incorporate multiple administrative, technical, and operational safeguards designed to reduce privacy risks while preserving the value of safety-relevant data. The following considerations illustrate one possible approach to achieving that balance.

Privacy by Design

Within a future framework, privacy protections would begin with data minimization. Researchers would receive only the data elements, time periods, and linkage capabilities necessary to conduct approved analyses. Whenever practical, research would be conducted using aggregate, de-identified, or pseudonymous data rather than direct identifiers. For studies requiring more detailed information, a future framework could apply a risk-based approach under which additional privacy protections, governance requirements, or legal authorizations could be introduced as data sensitivity increases.

Cybersecurity

A future framework could rely on secure research environments that incorporate encryption, role-based access controls, multifactor authentication, audit logging, and continuous monitoring. Access permissions would be limited to authorized project personnel, and all research activities would be subject to periodic review. Where appropriate, researchers would perform analyses within controlled computing environments that restrict data exports and reduce opportunities for unauthorized disclosure.

Interoperability and Data Quality

The usefulness of telematics data depends on consistent interpretation across manufacturers and research organizations. Accordingly, implementation of a future framework would include development of common data collection, data definitions, event taxonomies, metadata standards, and reporting conventions to improve comparability, reduce unnecessary duplication of effort, and support consistent interpretation of safety-relevant data across manufacturers and research organizations.

Transparency and Accountability

Public trust depends on transparency regarding how telematics data is collected, accessed, and used. Within a future framework, consumers would receive clear information about safety research activities, the protections governing those activities, and the limited circumstances under which vehicle-specific data could be accessed. Transparency and accountability would be supported through audit logging, periodic compliance reviews, incident reporting, and public transparency reports describing approved research activities, participating organizations, and program outcomes. Together, these measures would help demonstrate that vehicle-specific telematics data is being used consistently with approved transportation safety research objectives while maintaining appropriate protections for consumers and manufacturers.

Permitted Uses and Safeguards

Any future framework for responsible telematics data access will need to establish clear boundaries around how vehicle-specific data may be collected, accessed and used. Defining both permitted and prohibited uses is essential to maintaining public trust, protecting consumer privacy, and ensuring that the research pathway remains focused on improving roadway safety rather than serving unrelated commercial or governmental interests. Accordingly, any future framework would likely include clearly defined use restrictions alongside appropriate governance and oversight mechanisms.

Permitted Uses

Access to vehicle-specific telematics data would be limited to approved transportation safety research activities that demonstrably serve the public interest. Examples of research activities that could be supported under a future framework include:

- evaluation of advanced driver assistance systems and automated driving technologies;
- crash causation and injury prevention research;
- analysis of safety-critical and near-miss events;
- evaluation of vehicle software and safety system performance;
- assessment of roadway infrastructure, traffic operations, and safety countermeasures; and
- research supporting improvements to vehicle safety standards and transportation safety programs.

Approved projects would operate under clearly defined research protocols and would receive access only to the information necessary to accomplish those objectives.

Prohibited Uses

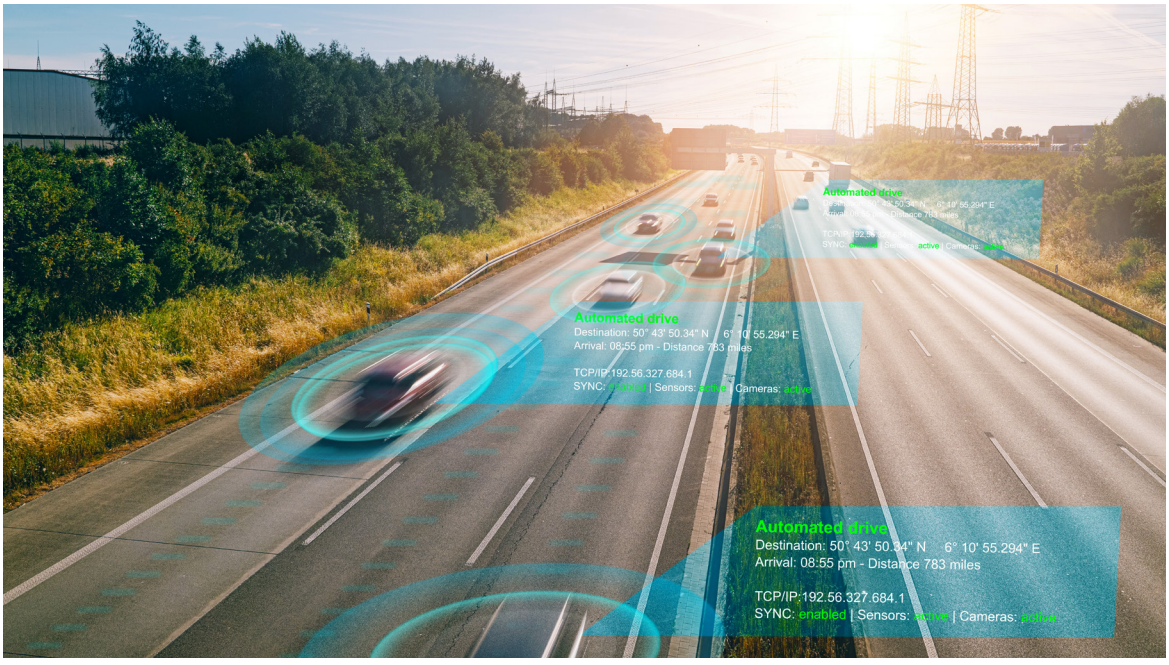
A future research access framework would not be intended to serve as a general-purpose vehicle data access program. Vehicle-specific telematics data obtained through the research framework would not be available for activities unrelated to transportation safety, including:

- advertising and marketing;
- insurance underwriting or pricing;
- driver scoring unrelated to approved research;
- employment or credit decisions;
- commercial profiling or analytics;
- routine law enforcement surveillance; or
- other unrelated commercial or governmental activities.

Similarly, any future research access framework would be designed to complement, rather than replace, existing legal processes governing civil litigation, regulatory investigations, or law enforcement access to vehicle data.

Reporting of Safety Findings

Although the future research access framework would be designed for research rather than regulatory enforcement, safety findings may have broader public benefit. When approved research identifies significant safety issues, findings could be communicated through existing safety reporting processes. Aggregated or appropriately de-identified information would be used whenever possible. This approach preserves the distinction between independent safety research and regulatory enforcement while ensuring that important safety insights can inform future transportation safety improvements.



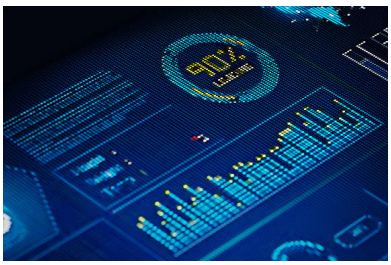
Implementation Considerations

Implementation of any future framework for responsible collection and access to vehicle-specific telematics data would likely require phased development through legislation, standards development, pilot programs, and continued collaboration among government, industry, academia, and other stakeholders. Successful implementation would require coordination among government agencies, vehicle manufacturers, standards organizations, researchers, and other stakeholders. Implementation could proceed incrementally through pilot programs and phased expansion, allowing governance processes, technical safeguards, and data standards to be evaluated and refined before broader deployment.

Pilot Programs

Pilot projects could provide an opportunity to evaluate governance processes, technical safeguards, data standards, and research workflows before broader implementation. Early pilots could focus on a limited number of manufacturers, research institutions, and transportation safety applications while evaluating privacy protections, operational costs, and research outcomes. Pilot programs would also provide opportunities to refine technical standards, improve interoperability, and build confidence among participating organizations before broader implementation.

Standards Development



Successful implementation would depend on common approaches to describing and exchanging vehicle safety data. Standards organizations, industry consortia, and government agencies could support these efforts by developing common event definitions, metadata standards, reporting conventions, and privacy-enhancing technical methods that improve interoperability while allowing manufacturers to preserve proprietary internal systems. Standardization also reduces research costs by improving comparability across manufacturers and reducing the need for project-specific data translation efforts.

Funding and Sustainability

Implementing and sustaining any future framework would require continued investment in independent transportation safety research. Costs associated with secure research environments, governance activities, standards development, and technical infrastructure could be allocated in a manner that is practical, transparent, and sustainable for participating organizations. Public-private partnerships, cooperative research agreements, and targeted federal funding may provide opportunities to support implementation while recognizing that improved roadway safety benefits both the public and private sectors.

Evaluation and Continuous Improvement

Any future framework would need to evolve alongside vehicle technology, privacy expectations, and transportation safety priorities. Periodic evaluation could assess research outcomes, security performance, governance effectiveness, and stakeholder experience while identifying opportunities to improve technical standards and operational procedures.

Conclusion

Vehicle-specific telematics data represents one of the most promising resources available for improving roadway safety. As vehicles become increasingly connected and software-defined, the ability to understand how vehicles operate under real-world conditions will become increasingly important for evaluating vehicle technologies, roadway infrastructure, and transportation safety programs.

The challenge is not whether vehicle-specific telematics data should contribute to transportation safety research, but how to enable responsible collection and access that maintains privacy, protects proprietary information, and preserves public trust. Addressing that challenge requires more than technical solutions alone. It also requires governance structures, legal safeguards, common standards, and clearly defined roles for government, industry, and the research community.

The concepts presented in this document illustrate one possible approach to enabling responsible access to vehicle-specific telematics data for transportation safety research. A future framework developed through legislation, standards development, and public-private collaboration could enable meaningful safety research while protecting privacy, safeguarding proprietary information, and maintaining public trust.

Although additional policy development, standards work, and pilot programs will be necessary before broad implementation, many of the technical, legal, and institutional building blocks already exist. Building on existing regulatory authorities, established privacy protections, and ongoing transportation safety programs provides an opportunity to responsibly expand access to vehicle-specific telematics data while maintaining the safeguards necessary to earn and sustain public confidence. Taken together, these existing capabilities provide a strong foundation for developing a future research access framework that advances transportation safety while preserving the privacy, security, and trust on which its long-term success depends.

This document was written by David Gorman (Principal, Surface Transportation Strategist) and was subsequently edited with assistance from MITRE's enterprise OpenAI environment hosted in MITRE's private cloud. All AI-assisted content was reviewed, validated, and edited by Becca Lehner (Program Manager, Surface Transportation), Kate Berman (Principal, AI Safety and Operations Intelligence and Assurance), Anthony Santago (Division Chief Engineer, Safety), and Michelle Michelini (Director, Surface Transportation) to ensure accuracy and compliance with MITRE's generative AI use guidelines.