PRIVACY POLICY RECOMMENDATIONS

Transportation systems in the U.S. rely on data to keep people and goods moving efficiently. Agencies use data to save lives, improve travel efficiency, and deliver better services. Digital tools can support economic growth and help agencies make smarter, data-driven investments.

Maintaining data privacy in an increasingly connected environment is critical to building public trust and ensuring transportation security. As new technologies improve safety and efficiency, policymakers must balance innovation with safety in developing regulations.

Transportation stakeholders across the public and private sectors follow strong guidelines and robust practices to minimize and anonymize collected and shared data. When Personally Identifiable Information (PII) is not necessary to provide a service or solution, agencies and companies should anonymize and aggregate data according to industry standards. PII should only be retained when necessary for essential functions, and organizations should follow best practices for privacy and data protection in its use, retention, and processing.[1]

The Intelligent Transportation Society of America (ITS America) supports federal efforts to establish a national data privacy framework with consistent standards across all 50 states. A patchwork of state and local privacy laws limits the widespread deployment of life-saving technologies that rely on accurate data.[2]

ITS America recommends the following privacy principles for ITS and the transportation sector:

☑ RESPONSIBLE DATA USE

Organizations should limit data collection to what is reasonably necessary for its intended purpose. A federal privacy framework should:

- When feasible, allow individuals to opt out of data collection, use, or sharing, and require consent before collecting and processing sensitive consumer data for personalized services, while preserving exceptions for beneficial data uses
- Clearly define the responsibilities of organizations that collect, use, and share data

Beneficial Data Uses: Federal privacy legislation must preserve organizations' ability to collect, use, process, and share transportation data that benefits consumers and communities, including reducing crashes and roadway fatalities, easing congestion, improving traffic operations, supporting law enforcement and emergency response, advancing transportation safety research, optimizing infrastructure design and construction, and processing payments.

[1] Such as these published by the National Institute of Standards and Technology (NIST) - Privacy Framework; Federal Trade Commission (FTC) - Business Guidance for Privacy and Security; and ITS America - Privacy Principles.
[2] ITS America Privacy Policy Recommendations

PRIVACY POLICY RECOMMENDATIONS

ITS AMERICA

PERSONAL DATA PROTECTION

Consumers should have rights over the collection, use, and sharing of their information. Organizations that collect, use, or share personal data must protect personally identifiable information. While transportation data is often anonymized and aggregated, individuals should be able to, under a federal framework:

- Know whether a company is collecting, using, or sharing their personal data
- Give or modify consent for data collection, use, and sharing when applicable and feasible
- Modify or withdraw consent when identifiable information is collected
- Obtain a copy of their personal information, when feasible and identifiable

Organizations should establish clear procedures and policies to protect stored data, follow privacy best practices,[3] and limit data collection to what is necessary for core operations that improve the transportation system.

ACCOUNTABILITY AND TRANSPARENCY

Federal privacy legislation should hold data users and collectors accountable while promoting transparency to prevent unethical practices and misuse of personally identifiable information. Organizations that collect and use data should publicly disclose:

PURPOSE OF DATA COLLECTION AND USE

CATEGORIES OF DATA BEING COLLECTED AND PROCESSED

CATEGORIES OF THIRD PARTIES WITH WHOM DATA IS SHARED

HOW CONSUMERS CAN EXERCISE THEIR RIGHTS

SECURITY

Organizations that collect, use, or share transportation data should implement strong cybersecurity practices, including incident response plans, compliance with applicable federal cybersecurity standards, employee training, and secure software systems. Congress should also require organizations to maintain comprehensive incident response plans to quickly address and mitigate data breaches and cyberattacks.

[3] See footnote 1.