ITS AMERICA

Privacy Policy Recommendations

ITS America Privacy Task Force

202.484.4847

www.itsa.org | info@itsa.org

1100 New Jersey SE Suite 850, Washington DC 20003

June 2025

Privacy Policy Recommendations

Transportation systems in the U.S. rely on the backbone of data to keep people and goods flowing easily and efficiently from place to place. Agencies are using data every day to save lives on their roads, improve efficiency of travel, and offer the best services possible. Digital tools can unlock economic growth and help transportation agencies make even smarter investments, all while relying on data to make informed decisions.

Maintaining data privacy in an increasingly connected and technology-enabled environment is critical to gaining public trust and upholding security in all modes of transportation. With all the safety and efficiency benefits that transportation technologies bring, balancing innovation and safety when crafting policies and regulations is essential.

Transportation stakeholders in both the public and private sector follow strong guidelines and have implemented robust practices to minimize and anonymize the data collected and shared. For use cases where Personally Identifiable Information (PII) is not essential to deliver the capability, service, or solution, public sector agencies and companies should anonymize and aggregate the data in accordance with industry norms. Only when it is impracticable to provide the functions without retaining some level of PII should it be kept. In such cases, adherence to best practices related to privacy and data protection, including, using, retaining, and processing PII, should be followed.[1]

The Intelligent Transportation Society of America (ITS America) supports Federal efforts to create a national data privacy framework. The transportation industry and its users flourish when there is certainty and reliability, and the same applies to data privacy protections for ITS and transportation technology. A patchwork of state and local data privacy laws hinders the ability for the effective widespread use of life saving technology that relies on accurate data. A federal privacy framework should be adopted that establishes uniform privacy standards across all 50 states.

ITS America recommends the following principles to guide a federal privacy framework as it applies to ITS and the transportation sector:

I. Responsible Data Use

Organizations should minimize the data collection to that which is reasonably necessary for the purpose of the use of the data. A Federal privacy framework should do the following:

- When feasible, allow individuals to opt-out of the collection, use, or sharing of data with exceptions for beneficial data uses (as described below)
- Provide clear and defined roles and responsibilities for those who collect, use, and share data

[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.

- Require that organizations obtain consent before collecting and processing sensitive consumer data for personalized services, with exceptions for beneficial data uses

Beneficial Data Uses: Any federal privacy legislation must preserve the ability of organizations to collect, use, process, and share transportation data that will provide broader societal benefit to consumers and communities – for purposes including, but not limited to: reducing vehicle crashes, reducing vulnerable road user injury and death; lowering traffic congestion and increasing efficiency; improving traffic management operations; supporting law enforcement; preventing, detecting, or responding to emergencies or other critical safety incidents; transportation safety research; optimizing infrastructure construction and design; and using payment data to complete transactions.

II. Personal Data Protection

Consumers should have rights with respect to the use, collection, and sharing of their information. Personally identifiable information must be protected by organizations that collect, use, or share personal data. While it is common practice for transportation data to be anonymized and aggregated, it is important that consumers have the ability to modify or withdraw consent to collection when that information is immediately identifiable. Under a federal framework individuals should be able to:

- 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 for the products and services you participate in
- Modify or withdraw consent for data collection in cases where information collected is identifiable
- Obtain a copy of their personal information when feasible and where information collected is identifiable

Organizations should establish clear procedures and policies for the protection of stored data, adhere to privacy best practices,[2] and limit data collection to that which is essential for core organizational practices that improve the transportation system.

[2] See footnote 1.

III. Accountability and Transparency

Federal privacy legislation must also hold data users and collectors accountable for their activities, while promoting a culture of transparency. This will prevent unethical practices and potential misuse of personally identifiable information. Those collecting and using data should share publicly:

- The purpose of data collection and use
- Categories of data being collected and processed
- Categories of third parties with whom they share data
- How consumers can exercise their rights

IV. Security

The security of data is essential to prohibiting the potential misuse of personally identifiable information and avoiding scenarios where data falls into the wrong hands. Organizations collecting, using, or sharing transportation data should establish and implement robust cybersecurity practices, including developing incident response plans, following applicable federal cybersecurity standards, conducting employee training activities, and investing in secure software systems.[3] Specifically, Congress should require organizations to develop and maintain comprehensive incident response plans to quickly address and mitigate data breaches or cyberattacks.

[3] See best practices in the NIST Cybersecurity Framework