

AUTOMOTIVE PRIVACY

Policy Priorities

1. Enact a National, Preemptive Consumer Privacy Law

Congress should enact a comprehensive federal privacy law that establishes strong, consistent protections for consumers in all 50 states and a single national compliance framework for regulated entities.

- Preemption is critical for the auto industry because vehicles are designed, manufactured, sold and operated across state lines, often crossing multiple jurisdictions in a single day. A patchwork of differing state requirements creates unnecessary complexity and uncertainty for consumers and manufacturers alike.
- A federal law should provide consumers with meaningful privacy rights, including:
 - Clear disclosures about data collection and use.
 - The right to know what personal information is collected and shared.
 - Meaningful consent rights, especially for sensitive data.
 - The right to access and delete certain personal information.
 - The right to opt out of profiling activities that may affect legal rights or access to critical services.

A single national standard would provide consumers with consistent protections, while enabling continued investment in vehicle safety, innovation and mobility.

2. Strengthen Protections for Sensitive Data

Consumers deserve enhanced protection when sensitive data is involved. Any federal privacy framework should clearly define what constitutes “sensitive data” and provide heightened requirements governing its collection, use, sharing, and sale, including clear consent mechanisms and disclosures. Strong protections for the most sensitive consumer data (e.g., health, precise geolocation, and biometric information) will enhance consumer trust, while providing confidence that such data is being used appropriately.

3. Preserve Data Use for Vehicle Safety and Innovation

Privacy laws should recognize that vehicle data is often collected and processed to support safety-critical functions. Policymakers should avoid strict data minimization requirements and ensure that automakers and suppliers can continue to use data to:

- Protect the safety of vehicle occupants and other road users.
- Provide services requested or reasonably expected by consumers.
- Identify and remedy safety defects and cybersecurity vulnerabilities.
- Support recalls, warranties, vehicle maintenance, and compliance with laws and regulations.
- Conduct research and development that enables the next generation of safer, smarter and more efficient vehicles.

4. Safeguard Trade Secrets and Confidential Business Information

Privacy legislation should not require automakers to disclose proprietary vehicle data, software, algorithms or other confidential business information to unaffiliated third parties.

- Mandated vehicle data-sharing frameworks raise significant concerns regarding consumer privacy, cybersecurity, and the protection of trade secrets and intellectual property. Such requirements could expose sensitive vehicle systems and competitively valuable information developed through substantial investment and innovation.
- Policymakers should ensure that any data privacy framework protects consumer privacy, while avoiding data access mandates that could undermine cybersecurity, innovation, and the integrity of vehicle systems.

5. Protect Domestic Violence Survivors from Connected Vehicle Abuse

Congress should enact targeted legislation, such as the Safe Vehicle Access for Survivors Act (H.R. 2110), to help domestic violence survivors quickly terminate or disable an abuser's access to their vehicle's location and connected services. The auto industry supports this legislation because it would provide a vehicle-specific solution that enhances survivor safety, while preserving the benefits of connected vehicle technologies.