Title I. Baseline Privacy Standards and Data Practices

Section 1: Title
This bill is entitled the "Autonomous Vehicle Information Act", or the "AVIA."

Section 2: Definitions
This section defines terms used in the bill.

Section 101: Operator Consent and Covered Entity Transparency
The manufacturer must contractually agree to explain the collection, sharing, and using of the operator's PII and the operator must opt-in to any or all PII collection practices to avoid a forced contractual agreement.

Section 102: Operator Control of and Access to Information
Autonomous vehicle manufacturers must provide the operators/users with the ability to view and edit their personally identifiable information which is collected. For example, an AV may know an operator's most frequently visited locations, and must allow an operator to make changes to this data at their convenience.

Section 103: Minimization, Retention, and Deletion
Autonomous vehicle manufacturers must not collect more data than is needed for legitimate business purposes, must obtain an operator's affirmative express consent to collect, share, or use such data, and must permanently delete such data as soon as it is no longer required for legitimate business purposes.

Section 104: Breach Notification and Mitigation
This section requires AV manufacturers to alert operators of any security or privacy breach, and take measures to mitigate the impact of the breach.

Section 105: Reasonable Security Safeguards and Biannual Audit and Update of Data Security Practices
This sections requires AV manufacturers to implement reasonable security safeguards and take biannual audits of their security, updating those found to be inadequate. These security safeguards include industry standard encryption mechanisms for all sensitive data at rest and in transit, as well as standard authentication mechanisms for granting valid parties access to the data.

As new security standards and vulnerabilities can appear with technological advances, the AV company must submit a biannual audit to the FTC ensuring its security practices are up-to-date. This provision ensures that the AV company maintains up-to-date software and requires a notification to the operator when the software is no longer compatible with the AV hardware.

Section 106: Data Practice Tax Deduction
Although 26 U.S.C. § 162 ought to and likely does permit industry to deduct data privacy costs as an "ordinary and necessary" business expense, this Act dispels any doubt to encourage companies to spend what they need to ensure robust data privacy security.

Section 107: Contracts with Third Parties
This section requires covered entities to ensure that any and all third-parties adhere to the Act as well. If the covered entity fails to do so, and the third-party incurs a breach, then both the covered entity and third-party are held liable for the breach.

Title II. Enforcement

Section 201: Rulemaking and Enforcement Authority
This section grants the Federal Trade Commission (FTC) the authority, in consultation with the National Highway Traffic Safety Administration (NHTSA), to issue privacy rules and regulations in accordance with the standards in this title, and to enforce against violations of both the statute and promulgated regulations. New FTC regulations must be issued within two years after passage of the bill. The FTC has been the chief federal agency on privacy policy and enforcement since the1970s. It has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information. Although the FTC's commitment to consumer privacy has remained constant, the Commission has employed different, though complementary, approaches to privacy over time, in part to account for changes in both technology and the marketplace. Thus, the FTC has the experience and the flexibility to address the pressing privacy security concerns posed by autonomous vehicles.

The section also creates a new authority for the FTC to enforce compliance. It provides that any violation of the Autonomous Vehicle Information Act ("AVIA") or regulations promulgated thereunder is an unfair and deceptive act or practice as defined under § 5 of the Federal Trade Commission Act. Enforcement under § 5 recognizes the FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act.

Section 202: Enforcement by State Attorneys General
This section grants State Attorneys General the authority to enforce the Autonomous Vehicle Information Act ("AVIA") and to obtain specified remedies on behalf of residents of their state harmed by alleged violations of the Act. This section also require state enforcers to notify the FTC in advance of filing a complaint, permit the FTC to intervene in the case, and restrict the states from suing on violations that are the subject of a pending federal enforcement action by the FTC.

Section 203: Preemption
This section clarifies that this statute and Federal regulations issued under its authority will preempt any conflicting state statutes or regulations.

Section 204: Private Right of Action
This section clarifies that the AVIA provides no private right of action for plaintiffs against those who violate the Act.

Section 205: Criminal Penalties
This section addresses criminal penalties for whoever wrongfully and intentionally access personally identifiable information. Under this section, penalties can be upwards of $50,000 in fines and 10 years in prison. Although conduct covered by this section is already illegal under the Computer Fraud and Abuse Act, this section offers stronger and more streamlined penalties.

Section 206: Report to the Commission
This section requires covered entities to submit an annual comprehensive report to the FTC certifying their compliance with this Act and the promulgated regulations.

Section 207: Effective Date
This section clarifies that this act is effective one year after enactment.