

DRAFT LEGISLATION

Vehicle Location Privacy and Fiduciary Accountability Act

An Act to prohibit the construction, procurement, and operation of networked automated vehicle surveillance systems that create comprehensive movement-tracking capacity; to establish fiduciary accountability for automated license plate recognition systems and similar technologies; to require real-time verification architecture that prevents retention of non-matching vehicle data; to prohibit retrospective location databases and cross-jurisdictional data aggregation; to impose fiduciary duties on private vendors operating surveillance infrastructure on behalf of government; to provide private rights of action and meaningful remedies for citizens whose vehicle location data is unlawfully collected, retained, or shared; and generally relating to vehicle location privacy and the constitutional prohibition on general warrants.

Prepared by Michael G. Leahy

Initial Draft | July 2026

Be it enacted by the [Legislative Body] as follows:

Section 1. Short title

(a) This Act may be cited as the "Vehicle Location Privacy and Fiduciary Accountability Act."

Section 2. Findings and purpose

(a) Findings

The [Legislative Body] finds that:

(1) Automated license plate recognition systems and similar vehicle identification technologies, when networked across multiple locations and operated with data retention capability, create comprehensive, discretionary, standing, and unaccountable surveillance capacity over the movement of all persons within the jurisdiction, regardless of whether any individual is suspected of criminal activity.

(2) Such networked surveillance capacity exhibits all four characteristics that the Founders condemned as the hallmarks of general warrants: perpetual duration through

indefinite data retention; universal scope through indiscriminate capture of all passing vehicles; discretionary executive power through warrantless query access by broad classes of officials; and delegable authority through cross-jurisdictional data-sharing agreements that extend access beyond any accountable chain of authorization.

(3) The constitutional violation inheres in the surveillance capacity itself, not in any particular exercise of that capacity. A system that photographs, catalogs, and retains the location of every vehicle that passes a camera has already accomplished the constitutional harm before any query is run, because the comprehensive record exists and is available for discretionary search.

(4) The plain view doctrine, which holds that observation of a license plate in public view does not constitute a Fourth Amendment search, does not authorize the construction of comprehensive retrospective movement databases from aggregated public observations. The distinction between observing a fact and systematically recording, retaining, and making searchable all such observations is the distinction between ordinary law enforcement and general surveillance.

(5) The privatization of surveillance infrastructure through vendor contracts does not diminish the constitutional concern. When a private entity builds and operates a comprehensive vehicle tracking network and makes the resulting data available to government agencies through subscription agreements, the constitutional analysis is identical to government operation of the same system. The private vendor is operating as a de facto governmental surveillance agent.

(6) Existing regulatory approaches, including data retention limits, use restrictions, and sharing agreements, are structurally insufficient because they regulate the exercise of surveillance power rather than eliminating the surveillance capacity that creates the constitutional harm. Architectural constraints, not procedural safeguards alone, are necessary to prevent the construction of digital general warrants.

(7) Real-time verification against active, particularized legal process (including active warrants, stolen vehicle reports, and Amber, Silver, and similar emergency alerts) is the only use of automated vehicle identification technology that is consistent with the duties government owes its citizens, because it is the only use that verifies a specific fact without building a comprehensive record. Where verification suffices, collection is constitutionally prohibited.

(8) The relationship between government and the people it serves is fiduciary in nature: government holds and exercises power in trust for the benefit of citizens, not for its own institutional convenience. When government collects, retains, or accesses personal location data, it acts as a fiduciary and owes duties of loyalty, care, and restraint to every person whose data it holds. This fiduciary obligation constrains what systems government may build, what data it may retain, and what access it may permit.

(9) The Supreme Court's recognition in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), that comprehensive location data implicates Fourth Amendment protections regardless of the third-party doctrine, and the Court's subsequent application of that

principle in *United States v. Chatree* (2026) to prohibit bulk location queries without individualized probable cause, confirms that networked vehicle surveillance databases are constitutionally suspect.

(10) Citizens can have no meaningful autonomy over their movements, associations, and daily lives when government holds, or can access through vendor contract, comprehensive records of where every vehicle in the jurisdiction has traveled, retained indefinitely and searchable without particularized justification.

(b) Purpose

The purpose of this Act is to:

- (1)** Prohibit the construction, procurement, and operation of networked automated vehicle surveillance systems that create comprehensive movement-tracking capacity within the jurisdiction;
- (2)** Establish that automated vehicle identification technology may operate only in real-time verification mode, comparing observed vehicles against active, particularized legal process without retaining data on non-matching vehicles;
- (3)** Prohibit the creation and maintenance of retrospective vehicle location databases, whether by government entities or private vendors operating on behalf of government;
- (4)** Impose fiduciary duties on private entities that collect vehicle location data and make it available to government, ensuring that the duties run directly to the persons whose data is collected and not merely to the government agency that contracted for the service;
- (5)** Provide enforceable private rights of action and meaningful remedies, including statutory damages, injunctive relief, and evidentiary exclusion, to citizens whose vehicle location data is collected, retained, or shared in violation of this Act; and
- (6)** Establish the principle that government's obligation to its citizens regarding surveillance technology is fiduciary: government may collect and use personal location data only in ways that serve the interests of the persons observed, not the institutional interests of government itself.

Section 3. Definitions

For the purposes of this Act, the following terms have the meanings indicated.

(a) "Automated Vehicle Identification System" or "AVIS" means any technology, including automated license plate recognition systems, optical character recognition cameras, vehicle fingerprinting systems, and similar technologies, that captures, reads, converts, stores, or transmits data identifying or capable of identifying a specific vehicle, including license plate numbers, vehicle make, model, color, distinguishing features, and associated location, date, and time information, through automated means rather than direct human observation.

(b) "AVIS Data" means any information generated, captured, or derived from the operation of an Automated Vehicle Identification System, including license plate numbers, vehicle descriptions, images, location coordinates, timestamps, and any analytical output produced by processing such data.

(c) "Active Legal Process" means a current, particularized judicial order, warrant, or statutorily authorized alert pertaining to a specifically identified vehicle, including active arrest warrants identifying a suspect vehicle, stolen vehicle reports, court-ordered vehicle location monitoring for a named individual, and Amber, Silver, Blue, and similar emergency alert designations. Active Legal Process does not include general investigative interest, intelligence gathering, pattern analysis, or any form of bulk or categorical authorization.

(d) "Real-Time Verification Mode" means a configuration in which an Automated Vehicle Identification System compares observed vehicle data against a list of vehicles subject to Active Legal Process and, when no match is found, immediately and irrevocably discards all data associated with the observation without creating any record of the non-matching vehicle's presence, identity, or location.

(e) "Retrospective Vehicle Location Database" means any database, data store, index, or collection of records, however denominated or structured, that retains AVIS Data from non-matching vehicles for any period beyond the real-time comparison required for verification against Active Legal Process, thereby enabling retrospective queries about the historical locations or movements of vehicles not subject to Active Legal Process at the time of observation.

(f) "AVIS Vendor" means any private entity that manufactures, operates, maintains, hosts, or provides access to an Automated Vehicle Identification System or AVIS Data, whether through sale, lease, subscription, data-sharing agreement, or any other commercial arrangement.

(g) "Network Aggregation" means the integration, linking, federation, or cross-referencing of AVIS Data from multiple collection points, jurisdictions, or operators into a system that enables queries across the aggregated data, whether through a centralized database, distributed query architecture, or any other technical means.

(h) "Government Entity" means any state, county, municipal, or local agency, department, board, commission, authority, or instrumentality, and any entity receiving public funds for public safety purposes, that deploys, operates, contracts for, or accesses an Automated Vehicle Identification System or AVIS Data.

(i) "Fiduciary Duty" means the legal obligation to act in the interest of the person to whom the duty is owed rather than in the interest of the duty-holder or any third party. For purposes of this Act, fiduciary duties include:

(1) The duty of loyalty: acting in the best interests of each person whose vehicle is observed, without self-dealing, opportunism, or subordination of those interests to the institutional interests of government or the commercial interests of any vendor;

(2) The duty of care: exercising reasonable diligence to protect vehicle location data from unauthorized collection, retention, access, disclosure, and misuse, and ensuring that system architecture prevents rather than merely prohibits the constitutional harms addressed by this Act;

(3) The duty of confidentiality: refraining from any unauthorized disclosure, sharing, sale, or secondary use of AVIS Data; and

(4) The duty of restraint: limiting data collection, retention, and use to the minimum necessary to accomplish the specific lawful purpose authorized by Active Legal Process, and refraining from building surveillance capacity beyond what that purpose requires.

(j) "Protected Person" means any natural person associated with a vehicle observed by an Automated Vehicle Identification System, regardless of whether the person is the registered owner, the driver, or a passenger. Every Protected Person has standing to enforce the rights established by this Act with respect to all AVIS Data derived from the observation of a vehicle with which that person is associated.

(k) "Hot List" means a list composed exclusively of vehicles subject to Active Legal Process, updated not less than every twenty-four hours, and purged of entries for which the underlying Active Legal Process has expired, been satisfied, or been withdrawn.

(l) "Vehicle Location Privacy Oversight Authority" or "Oversight Authority" means the body established by Section 9 of this Act to oversee compliance with and enforce the provisions of this Act.

Section 4. Fiduciary obligations regarding vehicle location data

(a) The relationship between government and the persons subject to automated vehicle surveillance is fiduciary in nature. Every Government Entity that deploys, operates, contracts for, or accesses an Automated Vehicle Identification System owes fiduciary duties, as defined in Section 3(i) of this Act, directly to every Protected Person whose vehicle is or may be observed by that system.

(b) Every AVIS Vendor that collects AVIS Data through systems deployed within this state, or that makes AVIS Data collected within this state available to any Government Entity, owes fiduciary duties directly to every Protected Person whose vehicle is observed by those systems. These duties run to the Protected Person, not to the Government Entity that contracted for the vendor's services. An AVIS Vendor may not discharge its fiduciary duties by complying with the terms of a government contract where those terms are inconsistent with this Act.

(c) The fiduciary duties established by this section are non-waivable and may not be disclaimed, limited, or transferred by contract, terms of service, or any other agreement. Any provision purporting to waive, limit, or disclaim the fiduciary duties owed to a Protected Person is void and unenforceable as against public policy.

(d) A Government Entity or AVIS Vendor that breaches any fiduciary duty established by this section is liable to each affected Protected Person under the private right of action and remedies provisions of Sections 11 and 12 of this Act.

Section 5. Prohibition on retrospective vehicle surveillance

(a) No Government Entity shall construct, procure, subscribe to, access, operate, fund, or maintain a Retrospective Vehicle Location Database. This prohibition applies regardless of whether the database is operated by the Government Entity directly, by an AVIS Vendor on behalf of the Government Entity, or by a third party to which the Government Entity has access through any contractual, cooperative, or informal arrangement.

(b) No Government Entity shall query, search, or request that any other entity query or search a Retrospective Vehicle Location Database on its behalf. An official, employee, or contractor of a Government Entity who queries a Retrospective Vehicle Location Database, or requests that another entity do so, commits a per se violation of this Act regardless of the purpose of the query.

(c) No AVIS Vendor shall create, maintain, or operate a Retrospective Vehicle Location Database using AVIS Data collected within this state, or collected by systems deployed within this state, regardless of where the database is physically located or hosted.

(d) The prohibitions of this section apply to AVIS Data regardless of whether it is stored in identified form, pseudonymized form, or any other format from which vehicle identity, owner identity, or location history could be reconstructed through combination with other available data.

Section 6. Permitted use: real-time verification only

(a) An Automated Vehicle Identification System may be operated by or on behalf of a Government Entity only in Real-Time Verification Mode, comparing observed vehicles against a Hot List composed exclusively of vehicles subject to Active Legal Process.

(b) When a vehicle observed by an AVIS operating in Real-Time Verification Mode does not match any entry on the Hot List, the system shall immediately and automatically discard all data associated with the observation. No record of the non-matching observation shall be created, retained, cached, buffered, logged, transmitted, or preserved in any form. System architecture shall ensure that non-matching data is irrevocably destroyed within the processing cycle and is not written to any persistent storage medium.

(c) When a vehicle observed by an AVIS operating in Real-Time Verification Mode matches an entry on the Hot List, the system may generate an alert to law enforcement and retain the matching observation record. The retained record shall include only the data necessary to identify the vehicle, the time and location of the observation, and the specific Active Legal Process that generated the match. Retained match records shall be subject to the audit trail requirements of Section 10 of this Act.

(d) Hot Lists shall be updated not less frequently than every twenty-four hours. Entries for which the underlying Active Legal Process has expired, been satisfied, been withdrawn, or is no longer current shall be removed at each update. No Government Entity or AVIS Vendor shall maintain a Hot List entry beyond the duration of the Active Legal Process that authorized it.

(e) Nothing in this Act prohibits a law enforcement officer from personally observing a license plate in the course of duties and acting on that observation consistent with applicable law. This Act regulates automated, systematic collection and retention, not individual human observation.

Section 7. Prohibition on network aggregation

(a) No Government Entity shall access, subscribe to, or participate in any system that aggregates AVIS Data from multiple jurisdictions, multiple operators, or multiple collection points into a searchable network, whether centralized or distributed. The prohibition applies to systems operated by AVIS Vendors, cooperative law enforcement networks, fusion centers, and any other arrangement that enables cross-jurisdictional or multi-point vehicle location queries.

(b) No AVIS Vendor shall offer, operate, or maintain a system that enables any Government Entity to query AVIS Data collected by systems operated by or on behalf of other Government Entities, other jurisdictions, or private operators, unless such query is limited to real-time Hot List verification and the system architecture ensures that non-matching data from other jurisdictions is never transmitted, displayed, or made available to the querying entity.

(c) Data-sharing agreements, mutual aid agreements, memoranda of understanding, and any other formal or informal arrangements that provide a Government Entity with access to AVIS Data collected by another Government Entity or by a private entity operating in another jurisdiction are void and unenforceable to the extent they provide access to retained AVIS Data. This subsection does not prohibit the sharing of real-time Hot List alerts for vehicles subject to Active Legal Process.

(d) No Government Entity shall circumvent the prohibitions of this section by requesting that a federal agency, another state's agency, a private entity, or any other intermediary query a networked AVIS database on its behalf. Such a request constitutes a violation of this Act by the requesting Government Entity.

Section 8. AVIS vendor obligations

(a) An AVIS Vendor that operates systems within this state shall configure those systems to operate exclusively in Real-Time Verification Mode when those systems are used by or on behalf of any Government Entity. An AVIS Vendor that maintains a Retrospective Vehicle Location Database containing data collected within this state, regardless of where that database is hosted, violates this Act and breaches its fiduciary duties under Section 4.

(b) A Government Entity that contracts with an AVIS Vendor remains jointly and severally liable for all violations of this Act and all breaches of fiduciary duty arising from the AVIS Vendor's conduct. The Government Entity's contract with the AVIS Vendor shall impose the full requirements of this Act on the vendor and shall provide for each Protected Person's enforcement rights as a third-party beneficiary of the contract.

(c) No AVIS Vendor shall enable, configure, or permit any default setting that shares AVIS Data collected within this state with any entity, jurisdiction, or system beyond those specifically and individually authorized in writing by the contracting Government Entity. Any default-on sharing configuration constitutes a per se violation of this Act and a breach of the duty of loyalty under Section 4. An AVIS Vendor that activates sharing without the contracting Government Entity's documented, affirmative, individualized authorization for each recipient is strictly liable for all resulting violations.

(d) An AVIS Vendor that reinstalls, reactivates, or continues to operate equipment within this state after a Government Entity has terminated its contract or ordered removal of the equipment commits a willful violation of this Act for each day the equipment remains operational, subject to enhanced penalties under Section 12(a)(4) and (a)(5) of this Act.

(e) An AVIS Vendor's obligations under this section arise at the moment of data capture and continue for as long as any AVIS Data collected within this state remains in the vendor's possession, custody, or control, regardless of the status of any contract with a Government Entity.

Section 9. Vehicle Location Privacy Oversight Authority

(a) There is established within [appropriate state agency or as an independent authority] a Vehicle Location Privacy Oversight Authority, which shall oversee compliance with this Act.

(b) The Oversight Authority shall have the following powers and duties:

(1) Investigate complaints filed by Protected Persons against Government Entities and AVIS Vendors;

(2) Conduct proactive audits of AVIS systems, including unannounced technical inspections of system configurations, data retention practices, and sharing arrangements, without requiring a prior complaint;

(3) Issue subpoenas for documents, data, system access, and testimony;

(4) Impose civil penalties up to [specified amounts] for violations of this Act;

(5) Issue cease-and-desist orders, remediation orders, and orders requiring system reconfiguration or data deletion;

(6) Refer matters to the [Attorney General] for criminal prosecution where violations are willful; and

(7) Certify AVIS system configurations as compliant with this Act, and revoke certifications upon a finding of non-compliance.

(c) The Oversight Authority shall be staffed by persons with demonstrated expertise in privacy law, information security, and surveillance technology. No person who has been employed by or served as a consultant to an AVIS Vendor within the preceding [five] years shall serve on or be employed by the Oversight Authority.

(d) The Oversight Authority shall submit annual reports to [the Legislative Body] disclosing: the number of AVIS systems in operation statewide; the results of all audits and investigations conducted; enforcement actions taken; complaints received and their disposition; and recommendations for legislative updates.

(e) Nothing in this section limits the enforcement authority of the [Attorney General] under Section 16 of this Act, or the private right of action available to Protected Persons under Section 11 of this Act.

Section 10. Audit and transparency requirements

(a) Every Government Entity that operates or contracts for an Automated Vehicle Identification System shall maintain a complete, tamper-evident, append-only audit log of all Hot List queries, all match alerts generated, all actions taken in response to match alerts, and all access to match records by any official, employee, or contractor.

(b) Audit logs shall record, at minimum: the identity of the person initiating or receiving each query or alert; the date, time, and location of the query or observation; the specific Active Legal Process justifying the query or Hot List entry; and the disposition of each match alert. Queries or searches that do not reference a specific, current item of Active Legal Process are prohibited, and a system that permits such queries violates this Act.

(c) Audit logs shall be retained for not less than five years and shall be available for inspection by the Oversight Authority, the [Attorney General], and any Protected Person exercising rights under Section 11 of this Act.

(d) Every Government Entity operating or contracting for an AVIS shall publish, not less than annually, a public report disclosing: the number of AVIS devices in operation; the number of Hot List match alerts generated; the number of match alerts resulting in enforcement action; the number of false-positive alerts; all entities with which AVIS Data has been shared and the legal basis for each sharing arrangement; and the results of any audit conducted under this section or by the Oversight Authority.

(e) Prior to initial deployment or renewal of any AVIS contract, a Government Entity shall conduct a public hearing with not less than [thirty] days' advance notice, at which the proposed system's technical architecture, data handling practices, sharing arrangements, and compliance with this Act shall be presented and subject to public comment. Deployment without the required public hearing is a per se violation of this Act.

Section 11. Private right of action

(a) Any Protected Person whose AVIS Data is collected, retained, shared, queried, or processed in violation of this Act may bring a civil action in [appropriate court] against any Government Entity, AVIS Vendor, or other person responsible for the violation. Actions may be brought individually or collectively as class actions.

(b) A plaintiff bringing an action under this Act need not demonstrate that the violation resulted in actual harm, economic loss, or misuse of the data. The collection or retention of AVIS Data in violation of this Act constitutes a per se injury to the Protected Person's constitutionally protected interest in freedom from comprehensive government surveillance of movement and association. Standing exists upon a showing that the plaintiff's vehicle was observed by an AVIS operating in violation of any provision of this Act.

(c) No pre-dispute arbitration clauses or class action waivers shall apply to actions under this Act. Any contractual provision purporting to waive the right to bring an action under this Act, or to require arbitration of claims arising under this Act, is void and unenforceable as against public policy.

(d) Actions may be filed without prior administrative exhaustion. The statute of limitations for actions under this Act is [five years] from the later of: (1) the date of the violation; or (2) the date the Protected Person discovered or reasonably should have discovered the violation. For violations involving concealed data collection, undisclosed sharing, or default-on configurations not authorized by the contracting Government Entity, the discovery rule tolls the limitations period until the Protected Person had or reasonably should have had actual knowledge of the violation.

Section 12. Remedies

(a) Available remedies

Courts may award in actions under this Act:

(1) Injunctive relief, including orders to cease operation of non-compliant AVIS systems, delete unlawfully retained AVIS Data, terminate non-compliant vendor contracts, remove AVIS equipment, and mandamus to compel compliance with the requirements of this Act;

(2) Compensatory damages for actual harms, including economic losses and harm from liberty infringements including surveillance, profiling, and chilling of associational and expressive freedoms;

(3) Statutory damages of not less than [five thousand dollars] per violation per Protected Person, scalable based on willfulness, duration, and the number of individuals affected. For purposes of this subsection, each unlawful retention of a non-matching vehicle observation, each unlawful query of a Retrospective

Vehicle Location Database, and each unlawful sharing of AVIS Data constitutes a separate violation;

(4) Enhanced statutory damages of not less than [twenty-five thousand dollars] per violation for willful violations, including operation of a Retrospective Vehicle Location Database with knowledge of this Act's prohibitions, unauthorized activation of data-sharing configurations, and failure to remove equipment after contract termination;

(5) Punitive damages for egregious breaches of fiduciary duty, including deliberate construction or maintenance of surveillance infrastructure in knowing violation of this Act, use of AVIS Data for immigration enforcement in violation of [applicable state law], and targeting of individuals or groups based on protected characteristics;

(6) Attorneys' fees and costs to prevailing plaintiffs; and

(7) Disgorgement of any revenue, profit, or other benefit derived by an AVIS Vendor from the unlawful collection, retention, or sharing of AVIS Data collected within this state.

(b) Equitable access

To address resource disparities between Protected Persons and defendants, courts shall:

(1) Provide expedited procedures for emergency injunctive relief in cases involving ongoing unlawful AVIS data collection, retention, or sharing;

(2) Waive filing fees for low-income Protected Persons upon sworn showing of financial need; and

(3) Apply a presumption in favor of class certification where the plaintiff establishes that the defendant's violation affected or is likely to have affected multiple Protected Persons through the same system, configuration, or practice.

(c) Government-specific remedies

For Government Entity violations, remedies include:

(1) Mandamus to compel compliance with specific provisions of this Act;

(2) Sovereign immunity waived for monetary awards up to [specified limits], paid from the operating budget of the responsible agency and not from the general fund; and

(3) Prohibition on indemnification of officers or employees found to have committed willful or knowing violations of this Act using public funds. Officers or employees who commit willful violations are personally liable for damages awarded under this section.

Section 13. Evidentiary exclusion

- (a)** AVIS Data collected, retained, or obtained in violation of any provision of this Act is inadmissible in any judicial, administrative, or legislative proceeding within this state, whether offered by a government entity or a private party. This exclusionary rule applies to the AVIS Data itself and to any evidence derived from or obtained as a result of the unlawfully collected, retained, or obtained AVIS Data.
- (b)** The inadmissibility provision of this section applies regardless of the good faith of the officer or entity that collected, retained, or obtained the data. The constitutional violation addressed by this Act is architectural; it cannot be cured by the subjective intent of any individual actor.
- (c)** In any proceeding in which AVIS Data is offered as evidence, the proponent of the evidence bears the burden of establishing, by a preponderance of the evidence, that the data was collected, retained, and obtained in full compliance with this Act. Failure to meet this burden results in exclusion.

Section 14. Private entity restrictions

- (a)** Private entities that collect vehicle location data for commercial purposes, including toll collection, parking management, insurance, fleet management, and repossession, owe fiduciary duties as defined in Section 3(i) of this Act to every Protected Person whose vehicle data they collect.
- (b)** No private entity shall share, sell, license, or make available AVIS Data to any Government Entity, except pursuant to a judicial order supported by probable cause and specifying particular vehicles. Bulk disclosure, standing data-sharing agreements, and subscription access by Government Entities to privately collected AVIS Data are prohibited.
- (c)** Private entities collecting AVIS Data for commercial purposes shall retain such data only as long as the specific commercial transaction requires, and in no event longer than [thirty] days after the transaction is completed. Aggregation of commercially collected AVIS Data into movement-tracking databases is prohibited.
- (d)** A private entity that violates this section is subject to the remedies and penalties of Section 12 of this Act and is liable for breach of fiduciary duty under Section 4.

Section 15. Government procurement restrictions

- (a)** No Government Entity shall enter into any contract, subscription, memorandum of understanding, data-sharing agreement, or other arrangement for Automated Vehicle Identification services unless:

 - (1)** The AVIS Vendor certifies, under penalty of perjury, that the system offered is architecturally configured for Real-Time Verification Mode and is incapable of creating, retaining, or transmitting data on non-matching vehicles;

- (2) The contract incorporates the full fiduciary duty regime and prohibitions of this Act as enforceable contractual terms;
 - (3) The contract designates each Protected Person as a third-party beneficiary with independent enforcement rights;
 - (4) The contract provides for immediate termination and equipment removal, at the AVIS Vendor's expense, upon any violation of this Act;
 - (5) The contract prohibits any default-on sharing configuration and requires documented, affirmative, individualized authorization for each entity granted access to any AVIS Data or system;
 - (6) The Government Entity has conducted the public hearing required by Section 10(e) of this Act; and
 - (7) The Oversight Authority has reviewed and approved the proposed system's architectural compliance with this Act.
- (b) Any contract entered in violation of this section is void ab initio. A Government Entity that operates an AVIS under a void contract commits a continuing violation of this Act for each day of operation.
- (c) Existing contracts for Automated Vehicle Identification services that do not comply with this Act shall be brought into compliance or terminated within [180] days of the effective date of this Act. During the compliance period, the Government Entity shall configure any existing system to operate in Real-Time Verification Mode and shall delete all previously retained AVIS Data on non-matching vehicles. Failure to comply within the [180]-day period constitutes a willful violation subject to the enhanced penalties of Section 12(a)(4).

Section 16. Enforcement

- (a) The Oversight Authority established by Section 9 of this Act shall have enforcement authority as specified in that section.
- (b) The [Attorney General] may bring an action in [appropriate court] to enforce any provision of this Act. The [Attorney General] may seek all remedies available under Section 12, including injunctive relief, civil penalties, and disgorgement.
- (c) A willful violation of Section 5 (prohibition on retrospective databases), Section 7 (prohibition on network aggregation), or Section 8(d) (continued operation after contract termination) by an officer, employee, or contractor of a Government Entity is a [gross misdemeanor/class A misdemeanor] punishable by [fine and/or imprisonment as specified].
- (d) Whistleblower protections: No Government Entity or AVIS Vendor shall retaliate against any officer, employee, or contractor who reports, in good faith, a violation or suspected violation of this Act to the Oversight Authority, the [Attorney General], or any

law enforcement agency. Retaliation includes termination, demotion, suspension, harassment, or any other adverse action. A person subjected to retaliation may bring a civil action for reinstatement, back pay, compensatory damages, and attorneys' fees.

Section 17. Relationship to federal law and interstate obligations

- (a)** No provision of this Act shall be construed to authorize any Government Entity to share AVIS Data with a federal agency in violation of [applicable state law restricting cooperation with federal enforcement]. AVIS Data collected within this state is subject to this Act regardless of any federal request, subpoena, or order, except as required by a valid federal court order following full adjudication of this state's sovereign interests.
- (b)** To the extent that a federal law, regulation, or court order requires conduct inconsistent with this Act, the Government Entity shall immediately notify the [Attorney General], who shall take appropriate legal action to defend this state's sovereign authority over the privacy of its residents.
- (c)** This Act applies to all AVIS Data collected within this state, regardless of where that data is subsequently stored, processed, or accessed. An AVIS Vendor that collects data within this state and transmits it to servers or databases located outside this state remains subject to this Act and to the jurisdiction of this state's courts for all purposes related to that data.

Section 18. Preemption of local law

- (a)** This Act establishes a statewide floor for vehicle location privacy protections. No local ordinance, resolution, or regulation shall authorize conduct that this Act prohibits.
- (b)** A county, municipality, or other political subdivision may adopt and enforce protections that are more restrictive than those established by this Act, including shorter retention periods for match data, additional procedural requirements for AVIS deployment, or outright prohibitions on AVIS within the subdivision's jurisdiction.

Section 19. Severability

- (a)** If any provision of this Act or its application to any person or circumstance is held invalid or unenforceable, the remainder of this Act and the application of its provisions to other persons or circumstances shall not be affected and shall continue in full force and effect.

Section 20. Effective date and transition

- (a)** This Act shall take effect [180] days after enactment, except that the private right of action under Section 11 shall be available for violations occurring on or after the effective date.

(b) During the [180]-day transition period, every Government Entity operating or contracting for an Automated Vehicle Identification System shall:

- (1)** Conduct an inventory of all AVIS systems in operation within its jurisdiction, including systems operated by AVIS Vendors on the Government Entity's behalf;
- (2)** Identify and delete all Retrospective Vehicle Location Database records containing AVIS Data on non-matching vehicles;
- (3)** Reconfigure all AVIS systems to operate in Real-Time Verification Mode;
- (4)** Terminate or renegotiate all AVIS Vendor contracts to comply with Section 15 of this Act;
- (5)** Disable all data-sharing configurations that provide access to AVIS Data beyond those specifically authorized under this Act; and
- (6)** Submit a compliance certification to the Oversight Authority and the [Attorney General] attesting to completion of the requirements of this subsection.

(c) An AVIS Vendor that has deployed equipment within this state shall cooperate with Government Entities in the transition required by this section. An AVIS Vendor that refuses to reconfigure systems, delete data, or remove equipment as required by a Government Entity acting in compliance with this Act is in willful violation of this Act.

Section 21. Construction

(a) This Act does not limit any right or remedy available to a citizen under the Fourth Amendment to the United States Constitution, Article [] of the [State] Constitution, applicable civil rights statutes, or any other provision of law. The rights and remedies provided by this Act are cumulative and in addition to all other rights and remedies.

(b) This Act shall be liberally construed to effectuate its purpose of protecting citizens from comprehensive government surveillance of their movements and associations through automated vehicle identification technology.

(c) Where a provision of this Act can reasonably be interpreted in more than one way, the interpretation that provides greater protection to the Protected Person shall govern.

Section 22. Funding

(a) The [state agency] shall allocate funds from [source] to support implementation of this Act, including:

- (1)** Establishment and staffing of the Vehicle Location Privacy Oversight Authority;
- (2)** Technical auditing capacity, including personnel and equipment necessary to conduct unannounced inspections of AVIS system configurations;

(3) Public education regarding the rights and remedies available under this Act; and

(4) Legal aid resources for low-income Protected Persons seeking to enforce their rights under this Act.

Section 23. Sunset review

(a) The Oversight Authority shall review this Act and report to [the Legislative Body] on its implementation, effectiveness, and recommended amendments every [five] years following the effective date. The review shall specifically assess whether the real-time verification requirement remains technically feasible and operationally adequate given developments in vehicle identification technology, whether additional categories of automated surveillance technology should be brought within the scope of this Act, and whether the remedies and penalties established by this Act are sufficient to deter violations.

About this draft

This is an initial draft of the Vehicle Location Privacy and Fiduciary Accountability Act, prepared as standalone legislation that may be enacted independently in any state. All bracketed provisions indicate items requiring legislative specification for the adopting state. This draft is prepared for discussion and does not represent the position of any government body.

For further information: fiduciarycommons.com | michael@fiduciarycommons.com