By: Bhojani H.B. No. 1167

A BILL TO BE ENTITLED

AN ACT

relating to the collection, use, retention, disclosure, and auditing of automated license plate reader data by employers of peace officers or fire fighters.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Chapter 411, Government Code, is amended by adding Subchapter T to read as follows:

SUBCHAPTER T. AUTOMATED LICENSE PLATE READER SYSTEMS

Sec. 411.601. DEFINITIONS. In this subchapter:

(1) "Automated license plate reader data" means a digitized image of a vehicle or license plate and associated information created or collected by an automated license plate reader system, including a license plate number, vehicle description, the date and time of a reading, and the location of a reading. The term does not include an ordinary dashboard-camera or body-worn-camera recording unless the recording is processed or indexed to create searchable license plate data.

(2) "Automated license plate reader system" means a fixed, mobile, or portable camera, software, or other equipment used, alone or in combination, to convert an image of a vehicle license plate into computer-readable data or to search, compare, store, or analyze the resulting data.

(3) "Audit log" means a record of an action taken by a user, agency, or vendor in accessing, querying, retaining,

exporting, disclosing, or deleting automated license plate reader data. The term does not include the underlying plate-read image or a database of vehicle sightings.

(4) "Department" means the Department of Public Safety of the State of Texas.

(5) "Employer" means the governmental entity that employs or appoints a peace officer or fire fighter as defined by Section 614.001.

(6) "Reasonable suspicion" means an objectively reasonable suspicion, based on specific and articulable facts and rational inferences from those facts, that a criminal offense is being committed or is about to be committed in the near or present future, and that an identified vehicle, its registered owner, or an occupant of the vehicle is materially connected to the suspected offense. The term does not include an unparticularized suspicion, a generalized desire to identify vehicles, or a mere hunch.

(7) "Vendor" means a private person or entity that, under contract with an employer, provides, operates, maintains, hosts, or has access to an automated license plate reader system or automated license plate reader data.

Sec. 411.602. APPLICABILITY; LIMITATIONS.

(a) This subchapter applies to an employer that operates, accesses, or obtains data from an automated license plate reader system and to a vendor acting on behalf of such an agency, regardless of whether the system or data is maintained on agency premises.

(b) This subchapter does not apply to a system used

exclusively for toll collection, enforcement of parking restrictions, or physical access control, if information from the system is not made available for a separate law enforcement purpose. An employer obtaining that information for a law enforcement purpose remains subject to this subchapter.

(c) This subchapter does not authorize any automated traffic enforcement practice otherwise prohibited by law or any search, seizure, or disclosure prohibited by the United States Constitution, the Texas Constitution, or other applicable law.

Sec. 411.603. AUTHORIZED USE; REASONABLE SUSPICION.

(a) An employer may use an automated license plate reader system only for a legitimate law enforcement purpose authorized by this section. The incidental collection of a plate image by an operating system does not, without more, authorize an individualized search or monitoring of that vehicle.

(b) Except as provided by Subsection (d), before an officer or other authorized user may search historical plate-read data for a particular vehicle or person, place a vehicle on a targeted alert list, or initiate targeted monitoring of the movements of a particular vehicle, the officer or user must possess reasonable suspicion and document:

(1) the specific and articulable facts supporting the suspicion;

(2) the connection between the identified vehicle and the suspected criminal offense; and

(3) the offense under investigation and an associated case, incident, or call-for-service number.

(c) The documentation required by Subsection (b) must be entered in the agency's designated system before the query or monitoring begins, except as provided by Subsection (e). The agency may not use automated license plate reader data to conduct general surveillance, monitor lawful activities without a permitted purpose, or create a record of an individual's movements without the authorization required by this section.

(d) The reasonable suspicion determination under Subsection (b) is not required for an action reasonably necessary to:

(1) execute a warrant or comply with an order issued by a court of competent jurisdiction;

(2) locate a vehicle or license plate reported stolen in a verified law enforcement database;

(3) locate a missing or endangered person on the basis of a documented report or officially issued alert;

(4) locate a person for whom an active arrest warrant has been verified through an authorized criminal justice database; or

(5) respond to an imminent threat of death or serious bodily injury when delay to obtain ordinary authorization would materially increase the danger.

(e) When the urgency of a situation described by Subsection (d)(3) or (5) prevents documentation before access, the officer or user shall document the basis for the access not later than 24 hours after the access. A supervisor who did not conduct the search shall review the record not later than 72 hours after the access.

(f) A positive match or alert generated by an automated

license plate reader system does not, standing alone, establish reasonable suspicion to stop or detain a person or vehicle. Before initiating a stop on the basis of an alert, an officer shall independently establish a lawful basis for the stop, visually confirm the displayed license plate when practicable, and verify the currency and accuracy of the underlying alert.

Sec. 411.604. RETENTION; PRESERVATION; DESTRUCTION.

(a) Except as provided by Subsection (b), an employer and its vendor shall permanently delete automated license plate reader data not later than the 30th day after the date the data was collected. Deletion must include copies, exports, and data accessible through a shared vendor platform.

(b) An agency may preserve specifically identified data beyond the period prescribed by Subsection (a) only if the data:

(1) was lawfully obtained and is reasonably necessary as evidence in an identified criminal investigation, prosecution, or court proceeding;

(2) is subject to a warrant, subpoena, court order, or legally enforceable evidence-preservation obligation; or

(3) is necessary to document a verified stolen-vehicle case, a missing-person investigation, or an emergency described by Section 411.603(d), and the agency records a particularized need for continued preservation.

(c) For each preservation under Subsection (b), an agency shall record the basis, the associated case or judicial-process number, the data preserved, the responsible officer, and the next review date. An agency shall review the continued need for

preservation at least once every 90 days and promptly delete data when the basis no longer exists, subject to applicable evidence-preservation and records-retention requirements.

(d) An agency may preserve only data material to the identified matter and may not use a preservation exception to retain an entire database, all readings from a camera, or indiscriminate travel histories. A recipient and a vendor must delete their copies within the same applicable period unless an independent lawful preservation basis is documented.

(e) An agency shall configure each system to enforce the retention and deletion periods automatically, maintain a verifiable record of deletions, and prevent recovery of deleted data in the ordinary course of system operations.

Sec. 411.605. DISCLOSURE; INTERAGENCY ACCESS; PROHIBITED SHARING.

(a) An agency may disclose specifically identified automated license plate reader data to another employer, a prosecuting attorney, or a court only if the disclosure is for a purpose authorized by Section 411.603, is otherwise lawful, and is approved in writing by a designated supervisor of the agency holding the data.

(b) Except as provided by Subsection (d), the request for disclosure must state:

(1) the requesting agency and the identity of the requesting officer or official;

(2) the offense, court proceeding, missing-person matter, or documented emergency for which the data is requested;

(3) the case number and the reasonable suspicion or specific exception relied on under Section 411.603;

(4) the particular data requested and the reason it is material to the stated purpose; and

(5) the name and approval of the releasing agency's designated supervisor.

(c) Before disclosure, the releasing agency shall record the recipient's agreement to use the data only for the stated purpose, protect the data from unauthorized access, prohibit further disclosure except as required by law or approved under this section, and comply with the applicable retention and destruction limits. An interagency agreement does not replace the case-specific authorization required by this section.

(d) An agency may make an otherwise lawful emergency disclosure without advance written approval to locate a missing or endangered person or address an imminent threat of death or serious bodily injury. The agency shall document the request and disclosure within 24 hours and obtain independent supervisory review within 72 hours.

(e) An agency or vendor may not:

(1) provide another agency or entity with unrestricted, continuous, or bulk access to data, or allow a general-purpose search of another agency's data without the case-specific authorization required by this section;

(2) sell, lease, license, or otherwise monetize automated license plate reader data;

(3) disclose data for a commercial, advertising, or

other purpose unrelated to the authorized matter; or

(4) permit a vendor to change sharing permissions or enable a new recipient without the express written approval of the agency that controls the data.

(f) The agency shall disable access by outside entities by default and maintain a record of each disclosure, including the data disclosed, recipient, stated purpose, authorizing supervisor, date, and method of transmission.

(g) An employer may acquire automated license plate reader data collected by a private entity other than an agency vendor only pursuant to a judicial warrant issued on probable cause, except to the extent disclosure is otherwise expressly required by state or federal law.

Sec. 411.606. ACCESS LOGS; SECURITY.

(a) An agency that uses or accesses an automated license plate reader system shall maintain a tamper-evident audit log of each query, access, alert-list change, preservation, export, disclosure, permission change, and deletion. The agency shall retain the audit log for at least two years.

(b) Each log entry must identify, as applicable:

(1) the name or unique user identifier and agency of the person taking the action;

(2) the date and time of the action;

(3) the type of action and search parameters, using masked identifiers to the extent consistent with a reliable audit;

(4) the specific authorized purpose, reasonable suspicion determination or exception, and related offense or case

number;

(5) the recipient and supervisor approving an export or disclosure; and

(6) any vendor access to the system or change to security or sharing permissions.

(c) The audit log may not be used to recreate a database of vehicle movements or to conduct a new criminal investigation through historical query records. An agency may access audit logs only for system security, compliance review, an investigation of misuse, or compliance with lawful judicial process.

(d) An agency shall use individual user credentials, access controls based on official duties, appropriate encryption and security protections, and prompt deactivation of credentials when a user is no longer authorized.

Sec. 411.607. PERIODIC AUDITS; CORRECTIVE ACTION.

(a) At least once every 12 months, each employer shall conduct and document an internal audit of compliance with this subchapter. The audit must review a risk-based sample of searches and disclosures, all reported incidents of suspected misuse, the completeness of access logs, compliance with retention and deletion requirements, and vendor access and sharing permissions.

(b) On discovering a material violation, the head of the agency shall promptly suspend the unauthorized access or disclosure, preserve relevant audit evidence, investigate the violation, and implement a written corrective action plan. The agency shall provide the department notice of a substantiated material violation and a summary of corrective action within 30

days after substantiation.

(c) The department may request records reasonably necessary to determine an agency's compliance, including policies, audit summaries, and evidence of corrected deficiencies. The department may require a written corrective action plan with reasonable deadlines, but may not obtain or disclose individual plate-read records except as necessary for a specifically authorized compliance investigation and subject to this subchapter.

Sec. 411.608. AGENCY POLICIES; USER TRAINING.

(a) An employer may not operate or access an automated license plate reader system unless the agency has adopted a written policy consistent with this subchapter and designated an employee responsible for the system's compliance and data security.

(b) The policy must address authorized purposes, reasonable suspicion documentation, emergency access, retention and preservation, interagency requests, user permissions, audit procedures, incident response, vendor responsibilities, and employee discipline for misuse.

(c) An agency shall publish its policy in a clear and conspicuous location on its public Internet website, excluding only information the disclosure of which would compromise system security or a specific ongoing investigation. An agency shall provide initial training before granting access and refresher training at least annually.

Sec. 411.609. VENDOR AGREEMENTS.

(a) An agreement under which a vendor processes automated license plate reader data for an agency must require the vendor to:

(1) act solely under documented instructions from the agency and recognize the agency's continuing control over the data;

(2) comply with the retention, access, logging, audit, and disclosure requirements of this subchapter;

(3) maintain technical controls that prevent unauthorized access, redistribution, aggregation, or use of the data for another customer;

(4) disable cross-agency sharing by default and obtain specific written approval for each change to sharing permissions;

(5) allow the agency to obtain complete audit records and verify deletion, including deletion from vendor-controlled copies;

(6) prohibit sale of data and prohibit use of data for product development or advertising without lawful, expressly authorized deidentification; and

(7) notify the agency without unreasonable delay, and not later than 48 hours after discovery, of a confirmed unauthorized access, disclosure, or loss involving agency data.

(b) A vendor may not provide direct access to an agency's data to another customer, government, or third party unless the disclosure has been approved by the agency under Section 411.605 or is required by law. A vendor agreement may not diminish an agency's obligations under this subchapter.

Sec. 411.610. REPORTING; PUBLIC TRANSPARENCY.

(a) Not later than November 1 of each year, an agency operating an automated license plate reader system shall submit to the department and publish on its website an annual report

containing, for the preceding state fiscal year, aggregated information concerning:

(1) the number of systems operated and searches performed;

(2) the number of disclosures to other agencies and the categories of recipient agencies;

(3) the number of records preserved beyond 30 days and the categories of preservation grounds;

(4) the number of verified incidents of unauthorized access or sharing and corrective actions taken; and

(5) the date and general findings of the most recent annual audit.

(b) The report may not identify a person, disclose vehicle-specific data, reveal an active investigative technique, or compromise an ongoing investigation or system security.

(c) Not later than February 1 of each year, the department shall publish an aggregate statewide report on compliance trends and recommendations. The department may prescribe a standardized reporting form to reduce administrative burdens on small agencies.

Sec. 411.611. CONFIDENTIALITY OF DATA.

(a) Automated license plate reader data and nonpublic, person-specific portions of audit logs obtained or maintained by an agency under this subchapter are confidential and are not subject to required public disclosure under Chapter 552.

(b) Subsection (a) does not prohibit disclosure in accordance with this subchapter, a court order, applicable criminal discovery obligations, or another law expressly requiring

disclosure. Written policies and aggregate reports required by this subchapter are public to the extent not otherwise confidential by law.

Sec. 411.612. RULES; COMPLIANCE.

(a) The Public Safety Commission shall adopt rules and model policies as necessary to implement this subchapter, including minimum requirements for documentation, secure access, preservation records, audit procedures, and annual reports.

(b) The department may refer a knowing, repeated, or material violation, or an agency's failure to implement required corrective action, to the attorney general. The attorney general may seek appropriate declaratory, injunctive, or other equitable relief to enforce compliance with this subchapter as authorized by law.

(c) This subchapter does not create a private cause of action for damages or waive sovereign or governmental immunity from damages. This subsection does not limit disciplinary action or any remedy independently available under other law.

Sec. 411.613. CONSTRUCTION.

(a) This subchapter establishes minimum requirements for the use of automated license plate reader data for law enforcement purposes. An agency may adopt more protective policies consistent with state and federal law.

(b) Nothing in this subchapter requires an agency to disclose data in violation of federal law, limits a defendant's right to discover evidence under applicable law, or authorizes a law enforcement officer to stop, search, or seize a vehicle without

the independent legal justification required for that action.

SECTION 2. Not later than March 1, 2028, the Public Safety Commission shall adopt the initial rules and model policies required by Section 411.612, Government Code, as added by this Act.

SECTION 3. An employer subject to Subchapter T, Chapter 411, Government Code, as added by this Act, shall comply with that subchapter not later than September 1, 2028. Not later than that date, the agency shall delete data collected before that date that would not qualify for continued retention under Section 411.604, Government Code, as added by this Act. The first annual report required by Section 411.610, Government Code, as added by this Act, is due November 1, 2029.

SECTION 4. This Act takes effect September 1, 2027.