Code of Virginia
Title 2.2. Administration of Government
Subtitle II. Administration of State Government
Part B. Transaction of Public Business
Chapter 55.6. Use of Automatic License Plate Recognition Systems

§ 2.2-5517. Use of automatic license plate recognition systems by law-enforcement agencies

A. For purposes of this section:

"Audit trail" means all records of queries and responses in an automatic license plate recognition system, and all records of actions in which system data is accessed, entered, updated, shared, or disseminated, including the (i) date and time of access; (ii) license plate number or other data elements used to query the system; (iii) specific purpose, as set forth in subsection D, for accessing or querying the system, including the offense type for any criminal investigation; (iv) associated call for service or case number; and (v) username of the person or persons who accessed or queried the system.

"Audit trail data" means all forms of data collected or generated by an automatic license plate recognition system for purposes of producing an audit trail.

"Automatic license plate recognition system" or "system" means a system of one or more high-speed cameras used in combination with computer algorithms to convert images of license plates, vehicles, or a combination of both into computer-readable data.

"Division" means the Division of Purchases and Supply of the Department of General Services.

"Law-enforcement agency" means any agency or entity that employs law-enforcement officers as defined in § 9.1-101.

"Missing or endangered person" means a person who has been identified as missing or endangered based on information provided by the National Criminal Information Center, the National Center for Missing and Exploited Children, or the Missing Children Information Clearinghouse (§ 52-31 et seq.) or pursuant to a Virginia Amber Alert (§ 52-34.1 et seq.), a Virginia Critical Operation for a Disappeared Child Initiative Alert (§ 52-34.3:1 et seq.), a Virginia Senior Alert (§ 52-34.4 et seq.), a Virginia Blue Alert (§ 52-34.7 et seq.), a Virginia Critically Missing Adult Alert (§ 52-34.10 et seq.), a Virginia Missing Person with Autism Alert (§ 52-34.13 et seq.), or any substantially similar alert under the laws of another state or territory of the United States, the District of Columbia, or the United States.

"Notification" means an alert from an automatic license plate recognition system that a license plate or vehicle matches a license plate or vehicle in a database utilized by the automatic license plate recognition system for comparison purposes.

"Person associated with human trafficking" means a person who is either a suspected victim or an alleged perpetrator of either commercial sex trafficking or labor trafficking.

"Publicly post" means to post on a website that is maintained by the agency or on any other website on which the agency generally posts information and that is available to the public or that clearly describes how the public may access such information.

"Query" means a search of automatic license plate recognition system data based on information entered by the user, including a full or partial license plate number, any identifying characteristics of a vehicle, the date, time, or location of an image, or any other data that is searchable within the automatic license plate recognition system.

"System data" means all forms of data collected or generated by an automatic license plate recognition system, including images of license plates, vehicles, any identifying characteristics of vehicles, the date, time, and location of an image, and any peripheral images collected from which analytical data may be extracted.

"Vendor" means a business, company, corporation, or other nongovernmental entity that contracts with a law-enforcement agency for the installation, use, or maintenance of an automatic license plate recognition system.

B. Pursuant to § 2.2-1112, the Division of Purchases and Supply shall determine the automatic license plate recognition systems for use in the Commonwealth in accordance with this section. An automatic license plate recognition system shall not be approved by the Division for use by a law-enforcement agency unless:

1. The vendor certifies that it will not sell or share any system data or audit trail data gathered in the Commonwealth, except upon request of the contracting law-enforcement agency for a purpose set forth in subsection F, and will only access system data or audit trail data upon request of the contracting law-enforcement agency for maintenance and quality assurance purposes;

2. The vendor certifies that its system is capable of purging system data collected or generated in the Commonwealth after 21 days of the date of its capture, or earlier if requested by the contracting law-enforcement agency, in such a manner that the system data is destroyed and not recoverable by either the vendor or the contracting law-enforcement agency;

3. The vendor certifies that its system is capable of producing an audit trail and purging audit trail data collected or generated in the Commonwealth after two years of the date of its capture in such a manner that the audit trail data is destroyed and not recoverable by either the vendor or the contracting law-enforcement agency;

4. The databases used by the system to provide notifications as set forth in subsection D are updated at least every 24 hours, or as soon as practicable after such updates become available; and

5. The system meets information security standards as established by the Virginia Information Technologies Agency.

C. (Effective July 1, 2026) A law-enforcement agency may enter into a contract with a vendor for the installation, use, or maintenance of a system approved by the Division. The contract shall specify that system data and audit trail data will be the property of the law-enforcement agency and that the system meets the requirements set forth in subsection B. The contract shall further specify that the vendor will immediately notify the law-enforcement agency upon receipt of any subpoena duces tecum, execution of any search warrant, or any other request from a third party for such system data or audit trail data, unless disclosure of such subpoena duces tecum, search warrant, or request is otherwise prohibited by law.

D. A law-enforcement agency may use a system only (i) as part of a criminal investigation into an alleged violation of the Code of Virginia or any ordinance of any county, city, or town where there is a reasonable suspicion that a crime was committed; (ii) as part of an active investigation related to a missing or endangered person, including whether to issue an alert for such person, or a person associated with human trafficking; or (iii) to receive notifications related to a missing or endangered person, a person with an outstanding warrant, a person associated with human trafficking, a stolen vehicle, or a stolen license plate. All information necessary for the creation of an audit trail shall be entered in order to query system data. A law-enforcement agency shall not query or download system data unless such data is related to at least one of these purposes. A law-enforcement agency may download audit trail data for purposes of generating audit reports. A stop of a motor vehicle based on a notification from the system shall be consistent with subsection M.

E. System data shall be purged after 21 days of the date of its capture in such a manner that such data is destroyed and not recoverable by either the vendor or the law-enforcement agency. Audit trail data shall be purged after two years of the date of its capture in such a manner that such data is destroyed and not recoverable by either the vendor or the law-enforcement agency. However, if the system data or the audit trail data is part of an ongoing investigation, prosecution, or civil action, such data shall be retained by the law-enforcement agency until (i) the investigation concludes without any criminal charges or (ii) the final disposition of any criminal or civil matter related to the data, including any direct appeals and any writs of habeas corpus pursuant to Article 3 (§ 8.01-654 et seq.) of Chapter 25 of Title 8.01 or federal law, in accordance with applicable records retention law and policy.

F. System data and audit trail data shall not be subject to disclosure under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). A law-enforcement agency shall not sell any system data or audit trail data. A law-enforcement agency shall not share system data or audit trail data with, or disseminate such data to, any database of any other state, federal, private, or commercial entity. A law-enforcement agency may share system data or audit trail data for the following purposes:

1. With another law-enforcement agency for purposes set forth in subsection D, which may include allowing another law-enforcement agency to query system data, provided that the agency receiving such data shall comply with all of the provisions of this section;

2. With the attorney for the Commonwealth for purposes set forth in subsection D or for complying with discovery or a court order in a criminal proceeding;

3. With a defendant or his counsel for purposes of complying with discovery or a court order in a criminal proceeding;

4. Pursuant to a court order or a court-issued subpoena duces tecum in any criminal or civil proceeding;

5. With the vendor for maintenance or quality assurance purposes; or

6. To alert the public to an emergency situation, a missing or endangered person, a person associated with human trafficking, or a person with an outstanding warrant.

In addition, the Department of State Police shall share system data obtained from any system installed, maintained, and operated on any limited access highway or any bridge, tunnel, or

special structure under the jurisdiction of the Commonwealth Transportation Board or the Department of Transportation with any law-enforcement agency in the locality where such system is installed, maintained, or operated, and such law-enforcement agency may share such system data for the purposes set forth in this subsection.

G. A law-enforcement agency that uses a system shall maintain records sufficient to facilitate public reporting as required by this section, the production of an audit trail, and discovery in criminal and civil proceedings, appeals, and post-conviction proceedings.

H. A law-enforcement agency that uses a system shall establish a policy governing such use that is consistent with this section that includes:

1. Training requirements for individuals who will use or access the system;

2. The purposes for which the system can be used or accessed;

3. Procedures to ensure that the databases used by the system to provide notifications as set forth in subsection D are updated at least every 24 hours, or as soon as practicable after such updates become available;

4. Procedures to confirm the accuracy of any notifications made by the system before stopping a vehicle that are consistent with subsection M;

5. A prohibition against downloading system data that is not related to at least one of the purposes set forth in subsection D, except for downloads of audit trail data for purposes of generating audit reports;

6. An internal auditing procedure that occurs at least once every 30 days;

7. Procedures for the retention and destruction of system data and audit trail data that are consistent with subsection E;

8. A prohibition on the sale of system data and audit trail data and restrictions on the sharing of system data and audit trail data that are consistent with subsection F; and

9. Security procedures to protect the system, system data, and audit trail data from unauthorized access, destruction, use, modification, or disclosure.

I. A law-enforcement agency that uses a system shall report to the Department of State Police by April 1 of each year, in a format to be determined by the Department of State Police, on its use of the system during the preceding calendar year, which shall include the following data:

1. The total number of cameras owned or leased by an agency as part of a system at the conclusion of each calendar year, including the number of such cameras designed to be affixed inside or on a motor vehicle, permanently affixed adjacent to a highway, or temporarily affixed or placed adjacent to a highway for purposes of capturing system data;

2. A list of all state and federal databases with which the system data was compared, unless the existence of any such database itself is not public;

3. The total number of times the system was queried, including the specific purposes of the queries, as set forth in subsection D, and the offense types for any criminal investigation;

4. The race, ethnicity, age, and gender of any individual identified as a suspect and charged with

a criminal offense as a result of a query of the system as part of a criminal investigation;

5. The number of motor vehicles stopped based on notifications from the system, including the specific reasons for the notifications as set forth in subsection D;

6. The race, ethnicity, age, and gender of the driver of any motor vehicle stopped based on a notification from the system;

7. Whether the agency allows any other law-enforcement agencies to access its system data, and if so, which other agencies have been granted such access;

8. The number of identified instances of unauthorized use of or access to the system, including the nature and circumstances of such instances; and

9. The number of subpoena duces tecum, search warrants, and any other requests received from a third party for system data or audit trail data, including the identity of the entity that requested the issuance of such subpoena duces tecum, executed such search warrant, or requested such data, and whether any data was provided to such entity, unless disclosure of such subpoena duces tecum, search warrant, or request is otherwise prohibited by law.

J. The Department of State Police shall aggregate the data provided pursuant to subsection I and report it to the Governor, the General Assembly, and the Virginia State Crime Commission by July 1 of each year.

K. A law-enforcement agency that uses a system shall publicly post the policy set forth in subsection H and the report set forth in subsection I. Data shall not be publicly posted if it contains personal or case identifying information. If any data (i) contains an articulable concern for any person's safety, (ii) is otherwise prohibited from public disclosure by federal or state statute, or (iii) may compromise sensitive criminal justice information if disclosed, such data may be excluded from being publicly posted.

L. A law-enforcement agency shall not use a system for the purpose of interfering with individuals engaged in lawful activities or tracking individuals on the basis of the content of lawfully protected speech.

M. A notification by a system for purposes set forth in subsection D does not, by itself, constitute reasonable suspicion as grounds for law enforcement to stop a vehicle. Prior to stopping a vehicle based on a notification, a law-enforcement officer shall:

1. Develop independent reasonable suspicion for the stop; or

2. Confirm that the license plate or identifying characteristics of a vehicle match the information contained in the database used to generate the notification.

N. Any person who willfully and intentionally queries, accesses, or uses a system for a purpose other than set forth in subsection D, or who willfully and intentionally sells, shares, or disseminates system data or audit trail data in violation of subsection F, is guilty of a Class 1 misdemeanor.

O. Any evidence obtained as the result of a violation of subsection D, F, L, or M is not admissible by the Commonwealth in any criminal or civil proceeding, but such evidence may be admitted by a defendant in a criminal proceeding or a litigant, other than the Commonwealth, in a civil proceeding.

P. This section does not apply to systems used:

1. For the enforcement of traffic laws, which includes parking regulations, speed limits, tolling requirements, high-occupancy vehicle requirements, or on-road emissions monitoring;

2. By the Department of Motor Vehicles at permanent weighing stations and in mobile weighing operations; or

3. By any state or local agency or any private entity for non-criminal justice purposes.

Q. A vendor shall immediately notify the contracting law-enforcement agency under subsection C upon receipt of a subpoena duces tecum, execution of a search warrant, or any other request from a third party for any system data or audit trail data, unless disclosure of such subpoena duces tecum, search warrant, or request is otherwise prohibited by law.

R. Prior to or coincident with the implementation of an automatic license plate recognition system, a local law-enforcement agency shall take measures to promote public awareness on the use of such system.

2025, c. 720.

The chapters of the acts of assembly referenced in the historical citation at the end of this section(s) may not constitute a comprehensive list of such chapters and may exclude chapters whose provisions have expired.