13.824 AUTOMATED LICENSE PLATE READERS.

Subdivision 1. **Definition.** As used in this section, "automated license plate reader" means an electronic device mounted on a law enforcement vehicle or positioned in a stationary location that is capable of recording data on, or taking a photograph of, a vehicle or its license plate and comparing the collected data and photographs to existing law enforcement databases for investigative purposes. Automated license plate reader includes a device that is owned or operated by a person who is not a government entity to the extent that data collected by the reader are shared with a law enforcement agency.

Subd. 2. **Data collection; classification; use restrictions.** (a) Data collected by an automated license plate reader must be limited to the following:

(1) license plate numbers;

(2) date, time, and location data on vehicles; and

(3) pictures of license plates, vehicles, and areas surrounding the vehicles.

Collection of any data not authorized by this paragraph is prohibited.

(b) All data collected by an automated license plate reader are private data on individuals or nonpublic data unless the data are public under section 13.82, subdivision 2, 3, or 6, or are active criminal investigative data under section 13.82, subdivision 7.

(c) Data collected by an automated license plate reader may only be matched with data in the Minnesota license plate data file, provided that a law enforcement agency may use additional sources of data for matching if the additional data relate to an active criminal investigation. A central state repository of automated license plate reader data is prohibited unless explicitly authorized by law.

(d) Automated license plate readers must not be used to monitor or track an individual who is the subject of an active criminal investigation unless authorized by a warrant, issued upon probable cause, or exigent circumstances justify the use without obtaining a warrant.

Subd. 3. **Destruction of data required.** (a) Notwithstanding section 138.17, and except as otherwise provided in this subdivision, data collected by an automated license plate reader that are not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection.

(b) Upon written request from an individual who is the subject of a pending criminal charge or complaint, along with the case or complaint number and a statement that the data may be used as exculpatory evidence, data otherwise subject to destruction under paragraph (a) must be preserved by the law enforcement agency until the criminal charge or complaint is resolved or dismissed.

(c) Upon written request from a program participant under chapter 5B, automated license plate reader data related to the program participant must be destroyed at the time of collection or upon receipt of the request, whichever occurs later, unless the data are active criminal investigative data. The existence of a request submitted under this paragraph is private data on individuals.

(d) Data that are inactive criminal investigative data are subject to destruction according to the retention schedule for the data established under section 138.17.

Subd. 4. **Sharing among law enforcement agencies.** (a) Automated license plate reader data that are not related to an active criminal investigation may only be shared with, or disseminated to, another law enforcement agency upon meeting the standards for requesting access to data as provided in subdivision 7.

(b) If data collected by an automated license plate reader are shared with another law enforcement agency under this subdivision, the agency that receives the data must comply with all data classification, destruction, and security requirements of this section.

(c) Automated license plate reader data that are not related to an active criminal investigation may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by this subdivision or other law.

Subd. 5. **Log of use required.** (a) A law enforcement agency that installs or uses an automated license plate reader must maintain a public log of its use, including but not limited to:

(1) specific times of day that the reader actively collected data;

(2) the aggregate number of vehicles or license plates on which data are collected for each period of active use and a list of all state and federal databases with which the data were compared, unless the existence of the database itself is not public;

(3) for each period of active use, the number of vehicles or license plates in each of the following categories where the data identify a vehicle or license plate that has been stolen, a warrant for the arrest of the owner of the vehicle or an owner with a suspended or revoked driver's license or similar category, or are active investigative data; and

(4) for a reader at a stationary or fixed location, the location at which the reader actively collected data and is installed and used.

(b) The law enforcement agency must maintain a list of the current and previous locations, including dates at those locations, of any fixed stationary automated license plate readers or other surveillance devices with automated license plate reader capability used by the agency. The agency's list must be accessible to the public, unless the agency determines that the data are security information as provided in section 13.37, subdivision 2. A determination that these data are security information is subject to in-camera judicial review as provided in section 13.08, subdivision 4.

Subd. 6. **Biennial audit.** (a) In addition to the log required under subdivision 5, the law enforcement agency must maintain records showing the date and time automated license plate reader data were collected and the applicable classification of the data. The law enforcement agency shall arrange for an independent, biennial audit of the records to determine whether data currently in the records are classified, how the data are used, whether they are destroyed as required under this section, and to verify compliance with subdivision 7. If the commissioner of administration believes that a law enforcement agency is not complying with this section or other applicable law, the commissioner may order a law enforcement agency to arrange for additional independent audits. Data in the records required under this paragraph are classified as provided in subdivision 2.

(b) The results of the audit are public. The commissioner of administration shall review the results of the audit. If the commissioner determines that there is a pattern of substantial noncompliance with this section by the law enforcement agency, the agency must immediately suspend operation of all automated license plate reader devices until the commissioner has authorized the agency to reinstate their use. An order of suspension under this paragraph may be issued by the commissioner, upon review of the results of the audit, review of the applicable provisions of this chapter, and after providing the agency a reasonable opportunity to respond to the audit's findings.

(c) A report summarizing the results of each audit must be provided to the commissioner of administration, to the chair and ranking minority members of the committees of the house of representatives and the senate

with jurisdiction over data practices and public safety issues, and to the Legislative Commission on Data Practices and Personal Data Privacy no later than 30 days following completion of the audit.

Subd. 7. **Authorization to access data.** (a) A law enforcement agency must comply with sections 13.05, subdivision 5, and 13.055 in the operation of automated license plate readers, and in maintaining automated license plate reader data.

(b) The responsible authority for a law enforcement agency must establish written procedures to ensure that law enforcement personnel have access to the data only if authorized in writing by the chief of police, sheriff, or head of the law enforcement agency, or their designee, to obtain access to data collected by an automated license plate reader for a legitimate, specified, and documented law enforcement purpose. Consistent with the requirements of paragraph (c), each access must be based on a reasonable suspicion that the data are pertinent to an active criminal investigation and must include a record of the factual basis for the access and any associated case number, complaint, or incident that is the basis for the access.

(c) The ability of authorized individuals to enter, update, or access automated license plate reader data must be limited through the use of role-based access that corresponds to the official duties or training level of the individual and the statutory authorization that grants access for that purpose. All queries and responses, and all actions in which data are entered, updated, accessed, shared, or disseminated, must be recorded in a data audit trail. Data contained in the audit trail are public, to the extent that the data are not otherwise classified by law.

Subd. 8. **Notification to Bureau of Criminal Apprehension.** (a) Within ten days of the installation or current use of an automated license plate reader or the integration of automated license plate reader technology into another surveillance device, a law enforcement agency must notify the Bureau of Criminal Apprehension of that installation or use and of any fixed location of a stationary automated license plate reader.

(b) The Bureau of Criminal Apprehension must maintain a list of law enforcement agencies using automated license plate readers or other surveillance devices with automated license plate reader capability, including locations of any fixed stationary automated license plate readers or other devices. Except to the extent that the law enforcement agency determines that the location of a specific reader or other device is security information, as defined in section 13.37, this list is accessible to the public and must be available on the bureau's website. A determination that the location of a reader or other device is security information is subject to in-camera judicial review, as provided in section 13.08, subdivision 4.

History: *2015 c 67 s 3*