HOUSE RESEARCH

Bill Summary

FILE NUMBER: H.F. 222 **DATE:** March 23, 2015
Version: Delete-everything amendment (H0222DE7)

Authors: Cornish and others

Subject: Automated license plate readers

Analyst: Matt Gehring, 651-296-5052

Overview

The bill regulates and classifies data related to use of automated license plate readers. Among other requirements, destruction of the data would be required within 30 days, if the data are not part of an active criminal investigation.

This bill also requires government entities to disclose the existence of certain types of surveillance technology.

A current temporary classification of automated license plate reader data, issued by the commissioner of administration, classifies the data as private or nonpublic. The temporary classification will expire August 1, 2015. After the temporary classification expires, automated license plate reader data will be presumptively public unless otherwise classified by law.

Section

1 **Arrest data.** Requires that the public data related to an arrest include data on whether an automated license plate reader was used as part of the arrest, unless that information would jeopardize an ongoing investigation. This disclosure is currently required when a wiretap or other eavesdropping technology is used.

2 **Use of surveillance technology.** Provides that the existence of all technology maintained by a law enforcement agency that may be used to record the activities of the general public, or of an individual or group of individuals, is public data.

3 **Automated license plate reader.** Regulates and classifies data related to automated license plate readers.

Section

Subd. 1. Definition. Defines "automated license plate reader."

Subd. 2. Data collection; classification; use restrictions. Restricts the types of data that may be collected from an automated license plate reader to:

(1) license plate numbers;

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

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

This subdivision also classifies automated license plate reader data as private data, unless a different classification is already provided in law (for example, if the data is active criminal investigative data).

It also prohibits use of databases beyond the Minnesota license plate data file for matching, unless the additional sources of data for matching relate to an active criminal investigation. A reader used to track a specific person is prohibited unless authorized by warrant issued upon probable cause.

Subd. 3. Destruction of data required. Requires destruction of data within 30 days, if it is not active criminal investigative data. An exception is provided if the agency receives a written request that the data may be used as exculpatory evidence in a criminal proceeding. These destruction requirements apply to the law enforcement agency that collected the data, and any other law enforcement agency that receives it.

An allowance for a participant in the Safe at Home address confidentiality program to request that the data be destroyed sooner is also provided. Data related to a Safe at Home request are private.

Inactive investigative data are subject to destruction according to the standard data retention schedule adopted by the agency.

Subd. 4. Sharing among law enforcement agencies. Requires a requesting law enforcement agency to meet the standards for seeking access to data as provided in subdivision 7. A receiving agency must comply with all requirements of the law related to data classification, destruction, and security.

Data may not be shared with, disseminated to, sold, or traded with any other entity unless explicitly authorized by law.

Subd. 5. Log of use required. Requires a log of use to be maintained by the law enforcement agency. The contents of the log are provided in the bill. The log is public, unless the agency determines the data are security data. A determination that the log is security data is subject to in camera judicial review.

Subd. 6. Annual audit. Requires an annual, independent audit to determine whether the data are properly classified or destroyed, and whether the agency has complied with the requirements of paragraph (g). Summary results of the audit are public, and must be provided to the commissioner of administration, the legislature, and the legislative commission on data practices and personal data privacy.

If a law enforcement agency is determined to be in a pattern of substantial noncompliance with the law, based on the results of the audit, the agency must suspend

Section

operation of automated license plate readers until the legislature has authorized reinstatement of their use. An order of suspension would be made by the commissioner of administration upon review of the audit results, the current law, and providing the agency an opportunity to respond.

Subd. 7. Authorization to access data. Requires law enforcement agencies to maintain automated license plate reader data consistent with standard data practices procedures, including notifications of security breaches.

The law enforcement agency must also adopt written procedures governing access to ensure that only those authorized, in writing on a case-by-case basis, by the agency head have access to the data, for a specific law enforcement purpose. An audit trail and training is required.

Subd. 8. Notification to Bureau of Criminal Apprehension. Requires law enforcement agencies to notify the Bureau of Criminal Apprehension (BCA) within ten days of installation or use of an automated license plate reader. The notification must include the fixed location of any stationary readers.

The BCA must maintain a public list of agencies using license plate readers, and locations of their use, on its website, unless the agency determines that the data are security data. A determination that the data are security data is subject to in camera judicial review.

Effective date. This section is effective August 1, 2015. Data collected before the effective date must be destroyed within 15 days of the effective date, if destruction would otherwise be required by this new law.

4 **Automated license plate reader policy.** Requires law enforcement agencies to adopt a written policy governing automated license plate readers. At a minimum, the agency's policies and procedures must include the requirements in law, including those provided in section 3 of the bill and the employee discipline standards for unauthorized access to data, provided under current law. The policy must be adopted no later than January 15, 2016.