

Department of Legislative Services
Maryland General Assembly
2025 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 516 (Delegate Korman)
Environment and Transportation

Motor Vehicles - Automated Enforcement Programs - Privacy Protections

This bill generally prohibits an “agency” (*i.e.*, a State police department, the State Highway Administration, a local police department, or another local agency that implements and operates an automated enforcement program) from accessing or using a recorded image or associated data without a warrant, subpoena, or court order unless the access or use is for an appropriate traffic enforcement purpose or law enforcement purpose. An agency that knowingly violates this requirement is subject to a fine of up to \$1,000 for *each* violation. The bill alters current statutory provisions by applying newly established standards and requirements for the use, processing, and disposal of recorded images (and associated data) to citations issued by automated enforcement systems in the State (*i.e.*, traffic control signal monitoring systems, automated railroad grade crossing enforcement systems, school bus monitoring systems, stop sign monitoring systems, speed monitoring systems, work zone speed control systems, bus lane monitoring systems, noise abatement monitoring systems, vehicle height monitoring systems, and any other automated traffic enforcement system authorized under State law). The bill also requires a custodian of recorded images produced by certain automated enforcement systems to deny inspection of the recorded images, subject to the bill’s changes. **The bill generally takes effect October 1, 2025, but accounts for the termination dates of stop sign and noise abatement monitoring system programs.**

Fiscal Summary

State Effect: The bill has an operational and potential fiscal impact on State law enforcement agencies, as discussed below. The Judiciary can likely handle any additional requests for warrants, subpoenas, or court orders with existing resources.

Local Effect: The bill has an operational and potential fiscal impact on local law enforcement agencies, as discussed below.

Small Business Effect: Potential minimal.

Analysis

Bill Summary: “Appropriate traffic enforcement purpose” is defined by the bill as the detection, investigation, or analysis of, or assessment or adjudication of liability for, a violation. “Violation” means a *traffic* violation that a *particular* automated enforcement system is intended to capture.

An agency *may* access and use a recorded image and associated data without a warrant, subpoena, or court order in exigent circumstances. Additionally, an employee or a contractor of an agency may access and use a recorded image and associated data (1) to audit or evaluate the accuracy of the automated enforcement system and (2) in a manner consistent with provisions of the bill requiring the removal and destruction of recorded images.

An agency must immediately remove from its records and destroy any recorded image or associated data captured under a program that does not constitute evidence of a violation. A recorded image or associated data captured under a program that *does* constitute evidence of a violation may be retained only for up to six months or until the conclusion of any criminal investigation or criminal or civil court action involving the recorded image or associated data. Before an agency removes and destroys a recorded image or associated data, the agency may disaggregate the data for analysis purposes in a manner that does not identify any individual.

An agency that implements and operates a program must adopt procedures relating to the operation of the program and the use of automated enforcement systems. The procedures must:

- identify the employee classifications in the agency that have authorization to access or use recorded images and associated data produced by an automated enforcement system;
- establish an audit process to ensure that information obtained through the use of an automated enforcement system is used only for appropriate traffic enforcement purposes and law enforcement purposes (as authorized in the bill);
- establish procedures and safeguards to ensure that agency personnel with access to recorded images and associated data are adequately screened and trained;
- establish procedures and safeguards for the secure storage of the recorded images and associated data (*i.e.*, prior to removal and destruction); and
- establish procedures for the removal and destruction of recorded images and associated data.

Recorded images and associated data must be stored using software that is independent from (and inaccessible to) other systems and networks. An automated enforcement system must be situated and focused in a manner that (1) captures recorded images and associated data of violations and (2) to the maximum extent possible, does not capture identifying images of the driver, other drivers or vehicles, or pedestrians. An automated enforcement system may not use biometric identifying technology, including facial recognition technology.

An agency or a contractor of an agency may not sell or otherwise transfer or share recorded images and associated data with another person other than (1) a person alleged to be liable for a civil violation recorded by an automated enforcement system; (2) a court of competent jurisdiction when adjudicating liability; or (3) another law enforcement agency for use only in an ongoing investigation. A law enforcement agency that receives recorded images or associated data pursuant to this sharing authorization is subject to the prohibitions and requirements established by the bill.

Current Law: State law currently authorizes the use of various automated enforcement systems, including traffic control signal monitoring systems, automated railroad grade crossing enforcement systems, speed monitoring systems, school bus monitoring systems, stop sign monitoring systems, bus lane monitoring systems, noise abatement monitoring systems, vehicle height monitoring systems, and work zone speed control systems.

Access to Public Records

Maryland's Public Information Act (PIA) establishes that all persons are entitled to have access to information about the affairs of government and the official acts of public officials and employees. Each governmental unit that maintains public records must identify a representative whom a member of the public may contact to request a public record. The Office of the Attorney General (OAG) must post all such contact information on its website and in any *Public Information Act Manual* published by OAG.

Duties of Custodians

Generally, a custodian of a public record must permit inspection of any public record at any reasonable time. A custodian must designate types of public records that are to be made available to any applicant immediately on request and maintain a current list of the types of public records that have been so designated. Each custodian must adopt reasonable rules or regulations that, consistent with PIA, govern timely production and inspection of a public record. Chapter 658 of 2021, effective July 1, 2022, requires each official custodian to adopt a policy of proactive disclosure of public records that are available for inspection under PIA, as specified.

Denials

Required Denials: A custodian must deny inspection of a public record or any part of a public record if (1) the public record is privileged or confidential by law or (2) the inspection would be contrary to a State statute, a federal statute or regulation, the Maryland Rules, or an order of a court of record. PIA also requires denial of inspection for specified personal and confidential records and information, including, for example, personnel and student records, hospital records, specified medical and financial information, and shielded criminal and police records. Chapter 62 of 2021 specifies that a record relating to an administrative or criminal investigation of misconduct by a police officer is not a protected personnel record under PIA and requires a custodian to allow access to such records by federal and State prosecutors. Chapters 548 and 549 of 2024 further specify that a record of positive community feedback that was not solicited by the police officer who is the subject of the feedback is not a protected personnel record under PIA.

Denials Related to Automated Enforcement Systems: Generally, a custodian must deny inspection of recorded images produced by (1) a traffic control monitoring system (red light camera); (2) a speed monitoring system; (3) a work zone speed control system; or (4) a vehicle height monitoring system. However, a custodian must allow inspection of recorded images (1) as required by the relevant authorizing statutes; (2) by any person issued a citation, or by an attorney of record for the person; or (3) by an employee or agent of an agency in an investigation or proceeding relating to the imposition or indemnification from civil liability under the relevant statutory provisions.

State/Local Fiscal Effect:

Fiscal Impact on State and Local Governments

The Department of Legislative Services advises that certain provisions of the bill (*e.g.*, the removal of records within specified periods and the establishment of procedures such as an audit process) may have a fiscal impact – specifically, there may be additional administrative costs for agencies that manage automated enforcement systems throughout the State. The Maryland Municipal League similarly advises of potential administrative costs.

The Judiciary advises that, although the bill may result in an increase for requests for a warrant, subpoena, or court order, any impact is not anticipated to significantly affect court operations.

Operational Impact on Law Enforcement Agencies

The Department of State Police and Prince George's County Police Department advise that the bill's limitations on the use of accessing or using a recorded image (or associated data) likely has an operational impact on law enforcement agencies. Under current law, for example, law enforcement agencies are generally able to retain recorded images and associated data even if there is no evidence of a traffic violation. In certain cases, the images/data may subsequently be used for other criminal investigations (*i.e.*, unrelated to a traffic violation). This practice may be significantly curtailed under the bill, given the general requirement to immediately remove recorded images/associated data that do not constitute evidence of a traffic violation. Although the bill authorizes a recorded image or associated data to be retained for up to six months (or until the conclusion of any criminal investigation or criminal or civil court action), the image must constitute evidence of a *traffic* violation (specific to the intended purpose of the camera that captured the image) in order to be retained by an agency. These requirements may limit the use of automated enforcement systems for other investigations.

Additional Information

Recent Prior Introductions: Similar legislation has been introduced within the last three years. See HB 1001 of 2024.

Designated Cross File: SB 381 (Senator Love, *et al.*) - Judicial Proceedings.

Information Source(s): Anne Arundel, Baltimore, Cecil, Frederick, Harford, and Prince George's counties; Maryland Municipal League; Judiciary (Administrative Office of the Courts); Department of State Police; Maryland Department of Transportation; Department of Legislative Services

Fiscal Note History: First Reader - February 20, 2025
km/jkb

Analysis by: Eric F. Pierce

Direct Inquiries to:
(410) 946-5510
(301) 970-5510