Marc Korman
Legislative District 16
Montgomery County

Chair
Environment and Transportation Committee

Rules and Executive Nominations Committee

The Maryland House of Delegates
6 Bladen Street, Room 251
Annapolis, Maryland 21401
410-841-3649
800-492-7122 *Ext.* 3649
Marc.Korman@house.state.md.us

THE MARYLAND HOUSE OF DELEGATES
Annapolis, Maryland 21401

Motor Vehicles – Automated Enforcement Programs – Privacy Protections (HB 516)

Testimony of Delegate Marc Korman - Favorable

Thank you, Madame Vice Chair and colleagues on the Environment and Transportation Committee. I come before you today to discuss the Automated Enforcement Privacy Act (HB 516). This legislation establishes a standard for the collection, use, auditing, and destruction of recorded images and associated data collected by automated enforcement programs. As we continue to use these automated enforcement programs for important safety goals, it is also critical that we maintain sensible guardrails. As you know, I am taking over this bill in the House from my now-Senate crossfire, Senator Sara Love. A version of this bill passed the House 105-32 last year.

Maryland currently has five different types of automated enforcement programs: school bus cameras, red light cameras, speed cameras, vehicle height monitoring cameras, and railroad grade crossing cameras. Additional systems, including work zone speed control systems, bus lane monitoring systems, noise abatement monitoring systems, and stop sign monitoring systems, have also been authorized in some jurisdictions. More automated enforcement programs are on the way as stop sign and noise cameras have previously been approved by the General Assembly for some pilot jurisdictions. Despite the extensive amount of data being collected by these programs around the state, there is no set standard for handling this data appropriately. This is further complicated by the fact that we do not have one centralized automated enforcement program. Instead, various law enforcement agencies at the state, county, and local level each have their own programs. With the increase in automated enforcement, the parameters outlined within this bill are necessary steps to protecting the privacy of citizens.

I have submitted a set of sponsor amendments reflecting bipartisan negotiations in the Senate. With these amendments, the chiefs and sheriffs are neutral on the legislation. The Automated Enforcement Privacy Act, with the amendments, would limit the use of images and recordings captured by automated enforcement programs to only traffic enforcement purposes except for certain circumstances. And these circumstances are important, as we have heard over the years compelling examples of where automated enforcement cameras have been used to investigate other, serious crimes. Specifically, an agency must request to use captured images and associated data through a formal documentation process subject to approval and limit usage to only the guideline of the request. In addition, the bill requires that agencies may only access recorded images with a warrant, subpoena, or court order, unless they are being used for traffic enforcement or law enforcement purposes directly related to traffic safety.

The bill includes a specific definition of ‘law enforcement agency,’ as stated in § 3–201 of the Public Safety Article, to clarify which entities are permitted to access recorded images under the exceptions outlined in the legislation. Any captured images or recordings that do not show evidence of a violation must be deleted immediately, ensuring that individuals captured are not identities in the process. Captured data applicable to a traffic violation may only be kept until the earlier of (1) one year following the conclusion of any criminal investigation or the exhaustion of all the avenues of adjudication for the violation, or (2) five years after the day on which the recorded image or associated data was captured. The bill also standardizes data handling under § 12–113.1 of the Transportation Article, in order to provide uniform requirements for processing, retention, and disposal across all enforcement systems.. The bill requires agencies to remain compliant by establishing employee training programs, designating auditors and standards, and following a formal destruction process for data. Automated enforcement systems may also not use biometric identifying technology such as facial recognition. It is important to set this framework in place to prevent the misuse and mismanagement of vital data.

To protect privacy and ensure oversight, the bill restricts public inspection of recorded images from automated enforcement systems, allowing access only in specific cases such as legal proceedings or review by cited individuals and their attorneys. It also requires local authorization and public hearings for certain programs, including stop sign and noise abatement monitoring systems, while limiting vehicle height monitoring systems to Baltimore City, Baltimore County, Harford County, and Prince George’s County, ensuring community input and proper oversight.

Regarding access by law enforcement, a law enforcement agency may access and use a recorded image or associated data already retained by the agency if (1) the agency documents a request that articulates a specific legitimate law enforcement purpose and (2) the custodian of the data maintains a written record of the request and whether it was granted. Once accessed, the agency may only use the recorded image or associate data for the purpose described in the request. Ultimately, any other law enforcement agency seeking access to the data must obtain an appropriate warrant, subpoena, or court order.

The Automated Enforcement Act will protect the privacy of citizens while ensuring our statewide systems can continue to protect and enforce necessary safety and traffic standards across the state. I urge a favorable report.