EPIC-Testimony-MD-HB1001-March-2024-Senate-Judicia
Uploaded by: Jake Wiener
Position: FAV

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

March 27, 2024

Maryland General Assembly
Senate Judicial Proceedings Committee
90 State Circle,
Annapolis, MD 21401

Re: Testimony of EPIC on House Bill 1001,

Dear Chair Smith, Vice Chair Waldstreicher, and Committee Members,

EPIC writes to urge you to advance H.B.1001, which would require sensible privacy protections when agencies deploy automated traffic enforcement systems like speed cameras and red-light cameras. More money than ever is now available for automated traffic enforcement systems through federal highway funding, and traffic enforcement systems are likely to expand across the country.[1] This is the time to put strong privacy protections in place so that traffic enforcement systems are not abused. H.B. 1001 would protect Marylanders by ensuring that automated camera systems are used to promote safe driving, not mass surveillance. While other states have enacted similar legislation in patchworks, Maryland has the opportunity to lead the nation by enacting a comprehensive bill that addresses the many ways municipalities might roll out automated traffic camera systems.

The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has long advocated for sensible limits on potentially dangerous surveillance technologies, particularly those which reveal location information.[3] EPIC studies advanced surveillance technologies including traffic enforcement systems and automated license plate readers, the flaws and dangers of these systems, and their impacts on society.[4]

As advocates for privacy and civil liberties, we are impressed with the core premise of this bill: that data from traffic enforcement cameras should be used for traffic safety, not leveraged for unjustified police activities or exploited by data brokers and bad actors. This bill protects Marylanders by limiting access to and use of images and data derived from automated enforcement systems to only traffic enforcement purposes and criminal investigations when police can obtain a warrant or court order, imposing strong limits on how long that data can be stored, and ensuring that agencies comply with those requirements through an audit process.

---

[1] Jenna Romaine, *States can now access billions for speed cameras under Biden's infrastructure law*, The Hill (Feb. 3, 2022), https://thehill.com/changing-america/sustainability/infrastructure/592689-states-can-now-access-billions-for-speed/.
[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] EPIC, *Location Tracking*, https://epic.org/issues/data-protection/location-tracking/.
[4] *See e.g.* EPIC, *Coalition Letter to DEA on unauthorized National License Plate Reader Program* (Mar. 8, 2023), https://epic.org/wp-content/uploads/2023/03/Coalition-Letter-DEA-ALPR-Program-March2023.pdf; *Kansas v. Glover*, 585 U.S. Brief of EPIC as Amicus Curie, (Sept. 6, 2019), https://epic.org/wp-content/uploads/amicus/fourth-amendment/glover/EPIC-Amicus-Kansas-v-Glover.pdf.

H.B. 1001 will be an effective protection for Marylanders because the bill requires four core concepts in data privacy: data minimization, purpose specification, data deletion, and auditing. By requiring cameras to minimize the amount of extraneous information they collect, this bill reduces the possibility that unrelated cars or passengers will be swept up in a system of mass surveillance. And by banning the use of facial recognition and biometric monitoring in automated cameras, the bill further ensures that these systems won't be used to do more than enforce Maryland's traffic laws. The bill further imposes a purpose specification, data can only be accessed for traffic enforcement purposes, not sold or transferred to other agencies where it might be abused. That purpose specification is reinforced through a data deletion requirement that ensures records will only be kept for long enough to substantiate a ticket—less data means less potential for abuse. And finally, all of those protections are enforced by training and auditing requirements, key provisions of any privacy protection.

H.B. 1001 is in line with laws regulating the use of specific automated traffic enforcement systems like those in Pennsylvania[5] and California,[6] but improves on those laws by addressing more types of automated systems and imposing higher data security provisions. This bill won't be the first in the country, but it will be the most comprehensive.

The warrant requirement in this bill aligns police processes for inspecting data from automated enforcement programs with the Constitution, and with existing procedures the police already use. Under the Fourth Amendment, police must generally obtain a warrant before performing a search. And police officers do this every day, whether they want to search a house or use a cell-phone hacking tool to unlock and inspect a cell phone that is already in police custody. In fact, officers regularly apply for warrants to search evidence held in police custody, from the contents of a locked briefcase, to a digital copy of an entire hard drive saved from a previous investigation. Both warrants and court orders are tools that police can readily apply for before accessing data from an automated enforcement program. Warrants are a pragmatic protection that simply ensure police have a good reason to perform a search, promoting meaningful police work while prohibiting harmful mass surveillance.

H.B. 1001 is not a ban on surveillance systems but a pragmatic check to ensure that municipalities don't evade existing regulations by using traffic enforcement as a fig leaf for mass surveillance. Maryland law already imposes some limits on general-purpose automated license plate readers, including a legitimate police use requirement and an audit requirement. MD. Public Safety Code § 3-509. H.B. 1001 prevents end-runs around Maryland's ALPR law and helps ensure that traffic enforcement systems will be deployed for traffic safety purposes.

---

[5] Pennsylvania Title 75 Pa.C.S.A. Vehicles § 3117 regulates red light cameras, requiring that images from those cameras may only be used for traffic enforcement of violations and requiring all images captured be deleted within one year, *available at* https://codes.findlaw.com/pa/title-75-pacsa-vehicles/pa-csa-sect-75-3117/.

[6] California Vehicle Code VEH § 40240 regulates car-mounted cameras for enforcing parking violations. The law requires cameras to minimize photographing unrelated cars or pedestrians, limits who can view parking enforcement images, and imposes a 60 day deletion requirement, *available at* https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=40240.&nodeTreePath=34.1.4&lawCode=VEH.

Furthermore, this bill reduces incentives to install systems where they could be abused. Traffic enforcement systems should be installed where they can reduce speeding and reckless driving, not where they can capture the most data from the most drivers, regardless of the impact on traffic safety. Confining the use of automated traffic camera data to traffic enforcement reduces the risk of mission creep. Mission creep is a serious threat to civil rights and good government that occurs when an agency expands the use of tools and information beyond the originally stated purpose and justification. More often than not the expansion is done in secret, without public approval, and to circumvent existing oversight and accountability measures. Here there is a risk that without privacy protections, traffic enforcement data will become a new source for mass surveillance, political policing, or over-policing. In other states license plate readers have been abused to track people's presence at protests,[7] monitor houses of worship,[8] and surveil immigrants against the wishes of local communities.[9] That means more police time spent on petty crimes, less time on meaningful public safety, and increased risks of wrongful arrest. When public safety agencies depart from their basic mission, harms to the public multiply while benefits decline.

Wrongful arrest and prosecution is a serious threat of any traffic enforcement system that lacks proper safeguards. Because these systems surveil the public, they can impact anyone. For example, without privacy protections, a system that misreads a license plate can incorrectly alert police to the presence of a wanted person and lead to innocent drivers being wrongfully pulled over, wrongfully arrested, or even wrongfully convicted based on an error in the system. This is not an unlikely scenario given license plate readers widely varying error rates, and field studies showing systems misreading license plates at disturbing rates as high as 37 percent.[10]

The potential harms from license plate readers and other traffic enforcement systems are multiplied when these systems are combined with already inaccurate databases, especially stolen vehicle registries. H.B. 1001 addresses this risk for traffic enforcement cameras by banning agencies from networking their automated ticketing systems with other databases. In one case from 2019, a rental car was mistakenly reported stolen so when Oakland, CA privacy activist Brian Hofer drove by an automated license plate reader with his family, the police were called.[11] Mr. Hofer was pulled over, police approached his car guns drawn, and detained him at length before concluding no crime had been committed. License-plate reader misreads led to the high-stakes wrongful detentions of Mark Molner in Kansas City, Denise Green in San Francisco, and Brittany Gilliam alongside her

---

[7] Rebecca Glenberg, *Virginia State Police Used License Plate Readers At Political Rallies*, Built Huge Database, ACLU (Oct. 8, 2013), https://www.aclu.org/news/national-security/virginia-state-police-used-license-plate-readers.

[8] *NYPD defends legality of spying on mosques*, CBS News (Feb. 24, 2012), https://www.cbsnews.com/news/nypd-defends-legality-of-spying-on-mosques/.

[9] Vasudha Talla, *Documents Reveal ICE Using Driver Location Data From Local Police for Deportations*, ACLU (Mar. 13, 2019), https://www.aclu.org/news/immigrants-rights/documents-reveal-ice-using-driver-location-data.

[10] A trial by the Vallejo Police Department in 2018 found that their stationary license plate readers made a mistake about 37 percent of the time. Jason Potts, *Research in Brief: Assessing the Effectiveness of Automatic License Plate Readers*, Police Chief Magazine (Mar. 2018), https://www.theiacp.org/sites/default/files/2018-08/March%202018%20RIB.pdf. When the Northern California Regional Intelligence Center, a police inter-agency center conducted a review of license plate reader data, they found about at 10 percent error rate across multiple agencies. Lisa Fernandez, Privacy advocate sues CoCo sheriff's deputies after license plate readers target his car stolen, Fox 2 KTVU (Feb. 19, 2019), https://www.ktvu.com/news/privacy-advocate-sues-coco-sheriffs-deputies-after-license-plate-readers-target-his-car-stolen.

[11] Charlie Warzel, *When License-Plate Surveillance Goes Horribly Wrong*, N.Y. Times (Apr. 23, 2019), https://www.nytimes.com/2019/04/23/opinion/when-license-plate-surveillance-goes-horribly-wrong.html.

four young daughters in Aurora, CO.[12] H.B. 1001 minimizes the risk of a wrongful detention or arrest from an automated traffic enforcement system by limiting the use to ticketing. Put simply, under this bill even if an automated traffic camera makes a mistake, the harm is a ticket, not an arrest.

Finally, EPIC encourages the legislature to fund and incentivize surveillance-free public safety interventions like safe-street design alongside any expansions to automated traffic enforcement systems. Well-designed streets and intersections naturally prevent speeding, protect cyclists, and improve the pedestrian experience. Those interventions reduce the need for traffic enforcement systems, and consequently reduce the risk of mass surveillance.

We urge the Committee to advance H.B. 1001 and provide Marylanders with meaningful privacy protections for traffic enforcement systems. Limiting the use of data derived from traffic enforcement can prevent wrongful arrests, harmful over-policing, and the sale of Marylanders' data to data brokers or out-of-state agencies.

Thank you for the opportunity to testify, please reach out with any questions to EPIC Counsel Jake Wiener at wiener@epic.org.

Sincerely,

Jake Wiener
Jake Wiener
EPIC Counsel

[12] Jonathan Hofer, *The Pitfalls of Law Enforcement License Plate Readers in California and Safeguards to Protect the Public*, The Independent Institute (Aug. 16, 2022), https://www.independent.org/publications/article.asp?id=14254#s3.

Senate HB 1001 Love written Transp Privacy.docx.pd
Uploaded by: Sara Love
Position: FAV

Sara N. Love
Legislative District 16
Montgomery County

Environment and Transportation
Committee

The Maryland House of Delegates
6 Bladen Street, Room 210
Annapolis, Maryland 21401
410-841-3454 · 301-858-3454
800-492-7122 *Ext.* 3454
Sara.Love@house.state.md.us

THE MARYLAND HOUSE OF DELEGATES
ANNAPOLIS, MARYLAND 21401

HB 1001 – Automated Enforcement Programs - Privacy Provisions

Chair Smith, Vice Chair Waldstreicher, Members of Judicial Proceedings –

Right now in Maryland law we allow a number of different automated enforcement programs:

- School bus cameras
- Red light cameras
- Speed cameras[1]
    - In school zones
    - In work zones
    - In residential areas (Anne Arundel, Montgomery, Prince George's)
    - On certain roads in certain places (e.g. I-83, Rte. 210, Jessup Rd., Oxford Rd.)
- Vehicle heigh monitoring cameras
- Railroad grade crossing cameras

Each year, we get a number of bills seeking to add to that list. This year alone we have bills to:

- Add Baltimore County to the residential camera program
- Expand the work zone camera program
- Enable a jurisdiction to add cameras on high-risk roads
- Enable a jurisdiction to add cameras on every traffic sign
- Enable three jurisdictions to use noise cameras
- Enable cameras on all buses to monitor: dedicated bus lanes, bike lanes, all bus stops, all curb cut-outs, double parking, all no-parking signs

This is a lot of automated enforcement, and a lot of data that is being collected. However, there is no statewide standard as to what is done with that data. HB 1001 would set that standard.

HB 1001 would put basic privacy parameters around this data, by setting retention/destruction time limits, limiting who would have access to the data, and requiring that the data be kept secure. In addition, it requires that the data only be used for traffic enforcement purposes, and that a system may not use biometric identifying technology, such as facial recognition.

With the explosion in surveillance technology, these are important parameters to put in place now.

I respectfully request a favorable report on HB 1001.

[1] Please note each of these have requirements and exceptions.

Department of State Police Position Paper HB 1001.

Uploaded by: Joey Sybert

Position: UNF

State of Maryland
Department of State Police

Government Affairs Unit
Annapolis Office (410) 260-6100

POSITION ON PROPOSED LEGISLATION

DATE: **March 27, 2024**

BILL NUMBER: **House Bill 1001** **POSITION: Oppose**

BILL TITLE: **Motor Vehicles – Automated Enforcement Programs – Privacy Protections**

REVIEW AND ANALYSIS

This legislation requires a law enforcement agency that operates an automated enforcement program to obtain a warrant, subpoena, or court order if the law enforcement agency needs to search the recorded images captured by the automated enforcement systems for any reason other than an appropriate traffic enforcement purpose. There is an exception for exigent circumstances. An agency shall immediately remove from its records and destroy any recorded image or associated data captured under the automated program if the image or records do not constitute evidence of a violation or all avenues of adjudication have been exhausted.

Under current law, the Department of State Police (DSP) works with our partners at the Maryland Department of Transportation for the collection of images collected by a Work Zone Speed Camera System. DSP is responsible for the review and approval of civil citations issued for violations.

House Bill 1001, by mandating that images can only be used for traffic enforcement, restricts a valid tool used by law enforcement to identify vehicles used in crimes or other offenses. Operationally, these cameras capture vehicle make and tag information. It also captures the location of the violation. The cameras do not capture the interior of the vehicle or driver. This legislation could negatively impact law enforcement agencies that may have a photo of a speeding vehicle or a vehicle running a red light near the scene of a major crime or other incident. Legitimate criminal investigations will be negatively impacted by the passage of this legislation.

House Bill 1001 requires a law enforcement agency to subpoena, obtain a warrant or court order to search its own records and recorded images from an automated enforcement program for any related investigation. This additional unprecedented step, requiring a police agency to serve a subpoena or warrant on itself, may jeopardize a timely response to a criminal investigation.

For these reasons, the Department of State Police urges the Committee to give HB 1001 an unfavorable report.

MCPA-MSA_HB 1001 Automated Enforcement Programs -

Uploaded by: Natasha Mehu

Position: UNF

Maryland Chiefs of Police Association

Maryland Sheriffs' Association

MEMORANDUM

TO: The Honorable William C. Smith, Jr., Chair and
Members of the Judicial Proceedings Committee

FROM: Darren Popkin, Executive Director, MCPA-MSA Joint Legislative Committee
Andrea Mansfield, Representative, MCPA-MSA Joint Legislative Committee
Natasha Mehu, Representative, MCPA-MSA Joint Legislative Committee

DATE: March 27, 2024

RE: **HB 1001 – Motor Vehicles - Automated Enforcement Programs - Privacy Protections**

POSITION: **OPPOSE**

The Maryland Chiefs of Police Association (MCPA) and the Maryland Sheriffs' Association (MSA) **OPPOSE HB 1001.** As amended, this bill would prohibit state and local police agencies or other agencies that operate an automated enforcement program from using recorded images or other data from the program without a warrant, subpoena, or court order unless the data is accessed for traffic enforcement or needed under exigent circumstances.

Automated enforcement cameras play a crucial role in traffic safety. They are used to deter people from speeding, running red lights, passing stopped school buses, or other traffic safety purposes and to penalize those who violate those laws. The goal is to ensure the safety of all who use our roads be it pedestrians, drivers, or bicyclists.

These cameras are also powerful tools that enhance public safety and aid law enforcement in solving crimes. Police investigators may use camera recordings and data to identify suspects on the run, track their movements, and reconstruct events. This bill would unnecessarily complicate law enforcement's ability to review the data as part of a criminal investigation when necessary.

As amended, law enforcement would only be able to access images and data for law enforcement purposes without a warrant, subpoena, or court order under exigent circumstances. While these amendments attempt to address some of the concerns that were previously raised regarding access to images or data for investigative purposes, they don't address all the issues. In many cases, law enforcement agencies are the owners of the data, therefore outside of exigent circumstances, they would be subpoenaing themselves for the data. This would add an unnecessary step in the process and burden limited judicial resources with simple internal data sharing.

Accessing this data for investigations is not something law enforcement takes lightly. Officers are not scanning automated camera footage in hopes of catching people in the act or doing so in place of other investigative methods. Prohibiting the use of the camera recording images and data from law enforcement investigations unless there is a warrant, subpoena, court order, or exigent circumstances may jeopardize timely response to crime and place individuals at further risk. For these reasons, MCPA and MSA **OPPOSE HB 1001** and request an **UNFAVORABLE** committee report.

532 Baltimore Boulevard, Suite 308
Westminster, Maryland 21157
667-314-3216 / 667-314-3236

HB1001 - TSO - Motor Vehicles Automated Enforceme

Uploaded by: Pilar Helm

Position: INFO

March 27, 2024

The Honorable William C. Smith, Jr.
Chair, Senate Judicial Proceedings Committee
2 East, Miller Senate Office Building
Annapolis MD 21401

Re: Letter of Information – House Bill 1001 – Motor Vehicles – Automated Enforcement Programs – Privacy Protections

Dear Chair Smith and Committee Members:

The Maryland Department of Transportation (MDOT) offers the following information on House Bill 1001 for the Committee's consideration.

The MDOT appreciates the sponsor's proactive collaboration on House Bill 1001. The intent of protecting consumers is currently built into the State Highway Administration's (SHA) contracts for Automated Enforcement – these contracts contain personally identifiable information protections. When license plates are photographed, there is a "zone of interest" that limits the viewable area to the rear of the vehicle and, for others, zoom in on the license plate. The photographs are not of the violators themselves.

The language of the bill does allow for data to be disaggregated for analysis purposes in a manner that does not identify any individual. As drafted, it may prove difficult to tie these violations back to serial offenders in the event Automated Enforcement violations are changed in the future to allow for a tiered fine structure based on multiple violations.

Finally, under the Maryland Public Information Act (PIA), MDOT is required to deny access to recorded images produced by certain automated enforcement systems as per § 4-321 of the General Provisions Article. House Bill 1001 creates a penalty for any employee who knowingly discloses records and assigns a fine up to $1,000 for a violation. While the intent is understandable, the imposition of personal liability against an employee, rather than the agency, may not be the best means of recourse.

The Maryland Department of Transportation respectfully requests the Committee consider this information when deliberating House Bill 1001.

Respectfully submitted,

Pilar Helm
Director of Government Affairs
Maryland Department of Transportation
410-865-1090

HB1001-JPR_MACo_LOI.pdf
Uploaded by: Sarah Sample
Position: INFO

MARYLAND Association of COUNTIES

House Bill 1001

Motor Vehicles – Automated Enforcement Programs – Privacy Protections

MACo Position:
LETTER OF INFORMATION

To: Judicial Proceedings Committee

Date: March 27, 2024

From: Sarah Sample

The Maryland Association of Counties (MACo) offers this **LETTER OF INFORMATION** on HB 1001. This bill limits the use of and access to images recorded by automated enforcement programs by law enforcement. It also mandates several procedures and requirements for automated enforcement programs run by local governments.

Automated enforcement programs are used for capturing motor vehicle violations in a variety of ways, as authorized by the State. Only a handful of jurisdictions have enabled some form of automated enforcement, and all are operated by a specified unit that oversees them within local law enforcement or transportation divisions. Each unit has established policies for how data is collected, reviewed, and stored. Some have standards above and beyond those identified in the legislation.

Counties appreciate the incredible need for privacy and security when it comes to data handling procedures, particularly records with identifying information of community members. It is a responsibility they do not take lightly as is evidenced by existing standards. The provisions of this bill intend to uphold the safety and security of this information and are well-meaning but, in a few narrow instances, potentially improbable.

For instance, red-light cameras are positioned to catch violations, often across multiple lanes. The bill's requirement to eliminate the capture of anything else in the area could present a significant challenge when the area to cover is sometimes in the range of 15 to 20 feet wide, with sidewalks on the adjacent edges of the street. Trying to exclude other drivers, vehicles, and potential pedestrians from the frame might not always be possible while also trying to ensure the cameras are able to catch the applicable violations.

Another primary concern is the requirement that these systems and software are not accessible to wireless networks. With dozens of cameras across some jurisdictions, remote data is uploaded everyday through wireless networks to the main servers of the automated enforcement unit. Manually collecting data from each of the cameras in remote locations could render some programs inoperable due to the sheer volume of staff and equipment those procedures would require.

All automated enforcement programs run by local jurisdictions are managed with extreme care and caution, as well as clear policies and training - which means most of the bill's specifications are part of existing procedures. Local governments appreciate the interest and intent of the legislation and for these reasons MACo opted to take no position and offer this **LETTER OF INFORMATION** on HB 1001.