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.