

ORDINANCE NO. _____

**AN ORDINANCE OF THE TOWN OF EASTON AMENDING CHAPTER 18 OF THE
TOWN OF EASTON CODE TO PROHIBIT AUTOMATED LICENSE PLATE
READERS, AUTOMATED VEHICLE SURVEILLANCE, AND THE COLLECTION,
ACCESS, USE, OR DISCLOSURE OF AUTOMATED VEHICLE SURVEILLANCE
DATA**

INTRODUCED BY: _____

WHEREAS, the Town of Easton is authorized by § 5-202 of the Local Government Article of the Annotated Code of Maryland to enact ordinances necessary to assure the good government of the municipality and to protect the health, safety, comfort, and welfare of its residents and visitors; and

WHEREAS, people have a reasonable interest in traveling upon public streets without the government or a private surveillance network automatically identifying their vehicles, recording their locations, and creating a searchable history of their movements; and

WHEREAS, automated license plate readers and substantially similar technologies collect information about every vehicle within their field of view, including vehicles whose owners and occupants are not suspected of any crime; and

WHEREAS, the continuous or systematic collection of vehicle-location information can reveal intimate details of a person's life, including visits to homes, workplaces, medical providers, houses of worship, political gatherings, schools, businesses, and associations with other persons; and

WHEREAS, being visible in public is not consent to the automated identification, recording, aggregation, retention, search, analysis, or disclosure of a person's movements; and

WHEREAS, the placement of surveillance equipment on private property does not eliminate the public consequences of a network designed to identify and track persons or vehicles traveling upon public streets and rights-of-way; and

WHEREAS, a prohibition limited to a particular manufacturer, product, trade name, camera design, or method of identifying a license plate could be evaded through changes in branding, ownership, hardware, software, analytics, or technical method; and

WHEREAS, an effective prohibition must apply to the surveillance capability, the resulting data, and direct or indirect access to that capability or data, regardless of who owns the equipment or where the information is stored; and

WHEREAS, ordinary doorbell cameras and premises-security cameras do not constitute automated vehicle surveillance merely because a vehicle appears in an image or because the system detects that an object is a vehicle, but a camera becomes part of an automated vehicle surveillance system when it is used to identify, index, search, compare, alert upon, aggregate, or track a particular vehicle or license plate; and

WHEREAS, the Town Council finds that targeted investigation based upon particularized facts does not require the indiscriminate automated collection of vehicle-location information concerning the general public; and

WHEREAS, the Town Council intends to prohibit the installation, operation, use, support, and facilitation of automated vehicle surveillance within the Town, and to prohibit the Town and every person acting under Town authority from obtaining the same surveillance information indirectly from another person, company, database, or governmental agency.

NOW, THEREFORE, the Town of Easton hereby ordains:

Section 1. The recitals set forth above are incorporated herein by reference and made a part of this Ordinance.

Section 2. Chapter 18 of the Code of the Town of Easton is hereby amended to add a new Article II, Sections 18-18 through 18-27, to read as shown on the attached Exhibit A.

Section 3. All Town departments, offices, agencies, boards, commissions, and instrumentalities shall, no later than the effective date of this Ordinance:

A. Cease all operation, use, access, and receipt prohibited by this Ordinance;

- B. Disable all accounts, credentials, alerts, integrations, and data-sharing arrangements involving an automated vehicle surveillance system or automated vehicle surveillance data;
- C. Terminate or decline to renew every contract, subscription, memorandum of understanding, intergovernmental agreement, trial, grant condition, or other arrangement authorizing conduct prohibited by this Ordinance, to the maximum extent permitted by law;
- D. Identify and secure all prohibited equipment and data pending lawful removal, return, destruction, or deletion;
- E. Request deletion of automated vehicle surveillance data previously supplied to or obtained by the Town, except to the limited extent preservation is required by a court order, applicable records-retention law, pending litigation hold, or an investigation or prosecution concerning a violation of this Ordinance; and
- F. Submit to the Town Clerk a written certification describing the actions taken to comply with this Section.

Section 4. If any section, clause, paragraph, sentence, phrase, or application of this Ordinance to any person, property, or circumstance is held invalid or unconstitutional by a court of competent jurisdiction, the invalidity or unconstitutionality shall not affect any other provision or application of this Ordinance that can be given effect without the invalid provision or application, and the provisions of this Ordinance are declared severable.

Section 5. In accordance with Article II, Section 9 of the Easton Town Charter, this Ordinance shall become effective twenty (20) calendar days after approval by the Mayor or passage of this Ordinance by the Council over the Mayor's veto.

Curry _____

Rankin _____

Montgomery _____

Davis _____

Abbatiello _____

I hereby certify that the above Ordinance was passed by a ye and nay vote of the Council this _____ day of _____, 2026.

Don Abbatiello, Town Council President

Delivered to the Mayor by me this _____ day of _____, 2026.

Kathy M. Ruf, Town Clerk

APPROVED:

Date: _____, 2026

Megan J. M. Cook, Mayor

EFFECTIVE DATE: _____, 2026

EXHIBIT A

ARTICLE II. AUTOMATED VEHICLE SURVEILLANCE

Section 18-18. Purpose and construction.

- A. The purpose of this Article is to prohibit automated vehicle surveillance within the Town of Easton and to prevent the Town, persons acting under Town authority, and private surveillance providers from constructing, maintaining, participating in, or obtaining the benefit of an automated system that records, identifies, indexes, searches, compares, analyzes, discloses, or tracks vehicles or license plates.
- B. This Article is prohibitory and shall not be construed as establishing permissible operating conditions, retention periods, approved uses, or a licensing system for automated vehicle surveillance.
- C. This Article shall be construed broadly to prevent circumvention by changes in manufacturer, ownership, branding, terminology, physical design, technical method, storage location, contractual arrangement, or division of functions among multiple persons or systems.

Section 18-19. Definitions.

For purposes of this Article, the following terms have the meanings stated:

- A. "Automated license plate reader" or "ALPR" means a fixed, portable, mobile, vehicle-mounted, handheld, airborne, or otherwise deployed camera, sensor, device, software application, service, or system that automatically or semi-automatically captures, reads, converts, interprets, records, or attempts to identify a license plate, registration plate, temporary registration, vehicle identification marking, or substantially similar vehicle identifier.
- B. "Automated vehicle surveillance data" means any image, recording, plate number, partial plate number, vehicle description, vehicle characteristic, date, time, location, direction of travel, alert, search result, metadata, inference, association, report, or other information obtained, generated, derived, inferred, or maintained through an automated vehicle surveillance system. The term includes copies, exports, screenshots, summaries, links, and information obtained from another person, governmental agency, data broker, contractor, or service provider.
- C. "Automated vehicle surveillance system" means any camera, sensor, imaging device, video system, optical system, software, algorithm, artificial intelligence system, database, network, service, or combination of hardware, software, data, or services that automatically or semi-automatically:
 - (1) Identifies or attempts to identify a particular vehicle, license plate, registration, vehicle occupant, or distinguishing vehicle characteristic;
 - (2) Creates, maintains, or contributes to a searchable record concerning the presence, location, date, time, direction, travel, or association of a particular vehicle or license plate;
 - (3) Compares a vehicle, license plate, image, or derived characteristic against a list, database, query, description, or other record;
 - (4) Generates or facilitates an alert, notification, match, lead, or search result concerning a particular vehicle or license plate; or
 - (5) Links, aggregates, or analyzes observations from one or more cameras, properties, accounts, locations, databases, or services to locate, follow, profile, or reconstruct the movements or associations of a vehicle or person.

The term includes an automated license plate reader and any substantially similar or successor technology, regardless of the name assigned by its manufacturer, vendor, owner, operator, or user.

- D. "Camera" includes a camera, doorbell camera, security camera, traffic camera, video system, sensor, or other device capable of capturing an image, recording, signal, or identifying information.
- E. "Covered Town person" means:
 - (1) The Mayor and every member of the Town Council;
 - (2) Every elected or appointed Town officer or official;
 - (3) Every employee of the Town, including police officers, civilian police personnel, utility employees, public works employees, department heads, supervisors, staff members, interns, and temporary employees;
 - (4) Every member, employee, or agent of a Town board, commission, committee, department, office, agency, authority, or instrumentality;

- (5) Every contractor, subcontractor, consultant, volunteer, or other person acting for, on behalf of, at the request of, under contract with, or under the direction or control of the Town; and
- (6) Any former covered Town person who retains, possesses, accesses, uses, or discloses equipment, credentials, information, or data obtained through service to the Town.
- F. "Fixed system" means an automated vehicle surveillance system installed, placed, stationed, or repeatedly deployed at or near substantially the same location, including a system mounted on a pole, building, sign, traffic-control device, utility structure, bridge, parking facility, trailer, tripod, portable mast, parked vehicle, or other structure or object. A system is fixed based on its operation and function, regardless of whether it can be moved.
- G. "Law-enforcement access" means any direct or indirect ability of a law-enforcement agency or law-enforcement personnel to request, search, retrieve, receive, view, download, analyze, obtain, or be alerted to a recording, image, data record, search result, or derived information.
- H. "Mobile system" means an automated vehicle surveillance system affixed to, carried by, transported by, or operated from a vehicle, aircraft, drone, handheld device, wearable device, or other movable platform. A mobile system that is stationed or repeatedly deployed at substantially the same location is also a fixed system.
- I. "Operate" includes activating, administering, controlling, configuring, maintaining, managing, monitoring, supporting, or causing a system or service to perform a function.
- J. "Person" means an individual, corporation, company, partnership, association, organization, property owner, tenant, governmental entity, public agency, contractor, service provider, or any other legal or commercial entity.
- K. "Premises-security camera" means a camera used primarily to protect or observe a particular residence, business, building, entrance, driveway, parking area, or other specific premises.
- L. "Surveillance service provider" means a person that manufactures, sells, leases, licenses, installs, hosts, stores, processes, supports, administers, operates, integrates, or provides access to a camera, automated vehicle surveillance system, surveillance network, analytics service, database, or associated data.
- M. "Town" means the Town of Easton, Maryland, and each of its departments, offices, agencies, boards, commissions, committees, authorities, and instrumentalities.

Section 18-20. General prohibition.

- A. Except for conduct expressly excluded under Section 18-24, no person shall knowingly purchase, acquire, own for use, possess for use, sell for deployment within the Town, lease, rent, install, place, activate, operate, maintain, manage, administer, host, support, fund, subscribe to, contract for, permit, authorize, facilitate, or otherwise participate in an automated vehicle surveillance system within the corporate limits of the Town.
- B. No person shall knowingly use a camera, recording, image, database, software application, analytics service, artificial intelligence system, or other technology to create, obtain, process, maintain, search, compare, analyze, aggregate, disclose, or transfer automated vehicle surveillance data concerning a vehicle observed within the Town.
- C. No property owner, tenant, occupant, manager, utility, or other person having authority over property or infrastructure within the Town shall knowingly permit the installation, placement, maintenance, or operation of an automated vehicle surveillance system upon that property or infrastructure.
- D. No person shall evade or attempt to evade this Article by:
 - (1) Describing an automated vehicle surveillance system as a security camera, traffic system, parking system, public-safety system, community-safety system, smart-city system, object-detection system, artificial intelligence service, or by any other name;
 - (2) Separating prohibited functions among multiple cameras, devices, companies, accounts, databases, agencies, or services;
 - (3) Locating storage, processing, analysis, personnel, or equipment outside the Town;
 - (4) Using a camera or data owned or controlled by another person;
 - (5) Obtaining an alert, report, screenshot, export, summary, or other derivative instead of raw data; or
 - (6) Using a successor, replacement, substantially similar, or technically modified system.
- E. When multiple components or persons collectively perform a prohibited function, each component and each person who knowingly performs, authorizes, facilitates, or materially supports that function is subject to this Article.

Section 18-21. Prohibitions applicable to the Town and covered Town persons.

- A. The Town shall not purchase, acquire, own for use, possess for use, lease, rent, install, place, activate, operate, maintain, manage, administer, host, support, fund, subscribe to, contract for, permit, authorize, or facilitate an automated vehicle surveillance system.
- B. A covered Town person shall not, in an official or personal capacity for any Town-related purpose, knowingly:
 - (1) Access, search, query, view, receive, obtain, download, copy, retain, disclose, share, transfer, analyze, or use automated vehicle surveillance data;
 - (2) Receive, subscribe to, act upon, or request an alert, match, notification, lead, report, or search result generated by an automated vehicle surveillance system;
 - (3) Enter, upload, submit, or cause the entry of a license plate, vehicle description, person, location, or other query into an automated vehicle surveillance system or database;
 - (4) Request, direct, encourage, authorize, assist, or knowingly permit another governmental agency, law-enforcement agency, contractor, vendor, private person, or service provider to perform an act prohibited by this Article;
 - (5) Use a personal account, personal device, unofficial communication, outside employment, third-party intermediary, or another jurisdiction to perform or obtain the benefit of an act prohibited by this Article;
 - (6) Accept complimentary access, a free trial, donated equipment, grant-funded access, vendor assistance, or an unsolicited search conducted for the purpose of avoiding this Article;
 - (7) Participate in a regional, statewide, interstate, federal, commercial, or private automated vehicle surveillance network, information-sharing arrangement, real-time crime center, law-enforcement portal, watchlist, or substantially similar system; or
 - (8) Renew, extend, amend, or enter into a contract, memorandum of understanding, policy, grant, agreement, or other arrangement that authorizes or facilitates conduct prohibited by this Article.
- C. No Town policy, departmental order, procurement, contract, memorandum of understanding, intergovernmental agreement, grant condition, emergency declaration, administrative approval, or direction from a Town official may waive or create an exception to this Article.
- D. No covered Town person may rely upon consent given by a camera owner, subscriber, vendor, property owner, or other person as authority to engage in conduct prohibited by this Article.

Section 18-22. Network surveillance, provider duties, and law-enforcement disclosure.

- A. No surveillance service provider shall knowingly use, process, aggregate, analyze, index, search, compare, disclose, transfer, or permit access to data obtained from a camera or sensor located within the Town for the purpose of identifying, locating, tracking, profiling, comparing, or generating an alert concerning a particular vehicle, license plate, person, or pattern of movement.
- B. No surveillance service provider shall knowingly permit a camera, sensor, account, recording, image, metadata record, or derived data originating within the Town to participate in:
 - (1) A law-enforcement request or disclosure system;
 - (2) A searchable camera or surveillance network;
 - (3) An automated vehicle, person, or object-location service;
 - (4) A regional, national, commercial, governmental, or private information-sharing system; or
 - (5) Any substantially similar system that permits searching, aggregation, automated identification, cross-camera analysis, alerts, or tracking.
- C. A surveillance service provider offering or supporting cameras or related services within the Town shall implement reasonable technical measures, including geographic exclusion where necessary, to prevent cameras and data originating within the Town from participating in conduct prohibited by this Article.
- D. Consent by a camera owner, subscriber, property owner, tenant, occupant, account holder, or service user does not authorize a surveillance service provider to conduct prohibited automated identification, aggregation, network searching, tracking, profiling, or law-enforcement access concerning persons, vehicles, or activities occurring on a public street, sidewalk, right-of-way, or property not lawfully controlled by the person giving consent.
- E. No surveillance service provider shall require a customer to waive the protections of this Article as a condition of purchasing or using a camera or related service.

Section 18-23. Data deletion, certification, records, and audit.

- A. A person possessing automated vehicle surveillance data collected, generated, obtained, or maintained in violation of this Article shall cease all use and disclosure of the data and shall permanently delete or destroy the data and all copies within thirty (30) calendar days after receiving written notice from the Town, unless preservation is required by a court order or other controlling law.
- B. The Town may require a surveillance service provider reasonably believed to operate, support, or process data from cameras within the Town to certify in writing that:
 - (1) Cameras and data originating within the Town are excluded from prohibited surveillance networks, searches, analytics, alerts, and law-enforcement access;
 - (2) Prohibited functions have been disabled for cameras and accounts within the Town;
 - (3) The provider has not knowingly disclosed automated vehicle surveillance data originating within the Town;
 - (4) Data required to be deleted under this Article has been deleted; and
 - (5) Software updates, default settings, integrations, and third-party services have not re-enabled prohibited functions.
- C. A certification required by this Section shall be signed under penalties of perjury by an officer or authorized representative having knowledge of the provider's compliance.
- D. Upon reasonable grounds to believe a violation has occurred, the Town may require a person subject to this Article to preserve and produce records reasonably necessary to determine compliance, including enrollment records, account settings, camera participation records, access logs, search logs, disclosure records, integration records, geofencing settings, retention records, and deletion records.
- E. Nothing in this Section authorizes the Town to obtain or review the substantive contents of private premises-security footage except to the minimum extent necessary to investigate a specific alleged violation and pursuant to lawful process.

Section 18-24. Exclusions and protected conduct.

- A. This Article does not prohibit:
 - (1) A person from visually observing a vehicle or manually recording or entering a license plate or vehicle description in connection with a particular incident;
 - (2) The use of a premises-security camera that records ordinary video or still images, provided neither the camera nor any associated system or service automatically or semi-automatically identifies, extracts, indexes, searches, compares, alerts upon, aggregates, or creates a searchable record concerning a particular vehicle, license plate, or vehicle movement;
 - (3) A camera or system that detects or classifies an object solely as a vehicle without identifying or attempting to identify the particular vehicle, license plate, occupant, or distinguishing characteristics, and without creating a searchable vehicle-location record;
 - (4) The owner or lawful user of a premises-security camera from personally selecting and voluntarily furnishing a particular recording relating to a specifically identified incident, complaint, or emergency, provided that the furnishing is not accomplished through a mass request, standing access arrangement, automated search, network search, vendor-mediated law-enforcement portal, or other prohibited system;
 - (5) The preservation, examination, or use of equipment or data solely as evidence in an investigation, enforcement action, judicial proceeding, or disciplinary proceeding concerning an alleged violation of this Article;
 - (6) A person who inadvertently or without solicitation receives prohibited data, provided that the person does not use or further disclose the data, promptly reports the receipt to the Town Clerk or other designated compliance official, and deletes or preserves the data only as directed for purposes of investigating the violation;
 - (7) Compliance with a final order issued by a court of competent jurisdiction, provided that the person complies only to the extent expressly required by the order; or
 - (8) The physical transportation of inactive equipment through the Town while the equipment is powered off, disconnected, and not used to collect, process, transmit, or receive data.
- B. No exclusion in this Section authorizes the operation of an automated vehicle surveillance system, the creation of automated vehicle surveillance data, or Town access to such a system or data.
- C. The person asserting an exclusion under this Section bears the burden of establishing that the conduct falls within the exclusion.

Section 18-25. Enforcement and penalties.

- A. A violation of this Article is a municipal infraction punishable by a fine of Five Thousand Dollars (\$5,000).
- B. Each prohibited camera, sensor, device, account, installation, data source, or surveillance node constitutes a separate violation.
- C. Each calendar day, or portion of a calendar day, during which a prohibited system remains installed, available, active, connected, supported, or capable of prohibited participation constitutes a separate violation for each camera, sensor, device, account, installation, data source, or surveillance node.
- D. Each prohibited access, search, query, request, alert, match, disclosure, transfer, download, copy, report, or use constitutes a separate violation.
- E. Each day that a person fails to delete data, disable access, produce a required certification, or comply with a lawful abatement order after the applicable deadline constitutes a separate violation.
- F. A materially false certification, statement, record, or representation made to conceal or deny a violation constitutes a separate violation.
- G. The Town may seek injunctive relief, abatement, removal of prohibited equipment, disabling of prohibited access, deletion of prohibited data, specific performance, recovery of enforcement costs where authorized by law, and any other remedy available at law or in equity.
- H. The Town may suspend, terminate, or decline to renew a contract, license, permit, approval, or business relationship with a person that knowingly violates this Article, to the extent permitted by law.
- I. No Town funds shall be used to pay, reimburse, indemnify, or otherwise satisfy a civil fine imposed personally upon a covered Town person for a knowing violation of this Article, except where payment is required by controlling law.
- J. A violation may be established without proof that the system produced an accurate identification, resulted in an arrest, or caused a separate injury. The prohibited collection, operation, access, disclosure, or participation is itself the violation.

Section 18-26. Discipline of covered Town persons.

- A. A knowing violation of this Article by a covered Town person constitutes gross misconduct, insubordination, misuse of public position, and conduct contrary to the public trust.
- B. Upon receipt of credible evidence that a covered Town person has committed a violation, the Town shall immediately suspend that person's access to law-enforcement databases, Town information systems, automated surveillance systems, and Town-issued equipment reasonably related to the alleged violation, and may reassign or suspend the person from related duties pending investigation.
- C. Following notice and the process required by applicable constitutional, statutory, contractual, collective-bargaining, personnel, or civil-service law, a sustained knowing violation by a Town employee constitutes grounds for termination and shall result in termination to the maximum extent permitted by law.
- D. A knowing violation by an appointed officer, board member, commission member, contractor, consultant, volunteer, or agent constitutes grounds for immediate removal, termination of appointment, termination of contract, or disqualification from further service, subject to any process required by law.
- E. A knowing violation by an elected official shall be referred to every authority having jurisdiction to investigate, censure, remove, prosecute, or otherwise act upon the misconduct.
- F. A person terminated or removed for a knowing violation shall not receive discretionary severance, a discretionary post-employment payment, a discretionary supplemental retirement contribution not already vested, or a post-employment consulting agreement from the Town.
- G. When conduct may constitute a crime, professional violation, ethics violation, or basis for pension forfeiture, the Town shall refer the matter and supporting evidence to the State's Attorney, Attorney General, Maryland Police Training and Standards Commission, applicable retirement system, ethics authority, licensing authority, or other body having jurisdiction.
- H. Following a conviction arising from a knowing violation committed through or in connection with public office or employment, the Town shall seek the maximum forfeiture, reduction, restitution, garnishment, or recovery of retirement or pension benefits authorized by Maryland law. Nothing in this subsection purports to forfeit a vested benefit without the judicial proceeding, conviction, findings, and process required by controlling law.
- I. An accidental or unsolicited receipt promptly reported and handled in accordance with Section 18-24(A)(6) is not a knowing violation.

Section 18-27. Whistleblower protection; no private waiver; future amendment.

- A. No person shall discharge, discipline, threaten, harass, discriminate against, or retaliate against another person for reporting in good faith a suspected violation, refusing to participate in prohibited conduct, preserving evidence of a suspected violation, or cooperating with an investigation or enforcement proceeding.
- B. No contract, employment agreement, account term, waiver, consent form, property agreement, policy, or private arrangement may waive or diminish the protections of this Article.
- C. No exception to this Article may be created administratively. Any exception or material narrowing of this prohibition requires amendment or repeal by ordinance following the same public legislative process required for adoption.
- D. Nothing in this Article shall be construed to authorize conduct otherwise prohibited by federal or State law or to limit any greater protection or remedy available under other law.