CITY OF NEW BEDFORD
JONATHAN F. MITCHELL, MAYOR

November 4, 2026

Council President Perreira and
Honorable Members of the New Bedford City Council
City Hall
133 William Street
New Bedford, MA 02740

Dear President Perreira and Members of the City Council:

I am submitting for the City Council's consideration the attached Ordinance amending Chapter 2 of the City Code to place greater restrictions on the employment of automatic license plate reader (ALPR) technology.

License plate readers are a powerful tool to promote public safety but they must be used responsibly. Reasonable limits on the technology's use are necessary to prevent misuse, protect legitimate privacy concerns, and enable the police to keep our City safe. The Ordinance reflects the Police Department's extensive review of emerging policies being developed across the nation to achieve these goals.

The measure includes several common-sense reforms: It requires all ALPR searches to be conducted by trained personnel and only for authorized public safety purposes. The Ordinance requires the City to delete all ALPR data not relevant to an open criminal or internal investigation after 30 days. It prohibits the sale, commercial exploitation, or unauthorized secondary use of ALPR data. And it sets up new NBPD procedures for reviewing allegations of unauthorized access of ALPR data.

Background

License Plate Reader (LPR) technology has been used by police departments around Massachusetts and the country since the early 2000s. Automatic license plate reader technology is still relatively new, becoming a mainstream law enforcement tool within the past few years. More than 6,000 other jurisdictions across the country had already signed agreements with Flock and other ALPR companies before the NBPD did so. The NBPD adopted Flock Safety's ALPR technology in December 2024.

ALPR technology has proven invaluable for thousands of police departments, including in New Bedford, allowing the NBPD to locate stolen vehicles, identify vehicles associated with serious crimes, and find missing or endangered people. ALPR technology has contributed to the NBPD's efforts to keep the City safer by providing officers with the tools they need to monitor city streets without having to have an officer posted on every corner. In March 2025, ALPR technology was used to track down Wilo Morales Colon, a New Bedford resident who was wanted following the death of Karina Martinez-Ortiz, outside Springfield, Massachusetts. ALPR technology was also vital during the manhunt for the Brown University shooter in December 2025.

In recent months, New Bedford residents have voiced reasonable concerns about privacy and misuse during the rise of ALPR technology. Police Chief Jason Thody ordered a comprehensive audit of the NBPD's use of Flock technology on July 31 and shut down all Flock cameras citywide on August 11.

The resulting audit, which examined Flock searches in 2026, contributed to the firings of two officers and the NBPD's decision not to renew its contract with Flock Safety when it expires on November 12. The results of the continuing audit, which is reviewing Flock searches between December 20, 2024, the day Flock's technology was adopted by the NBPD, and December 31, 2025, will be announced upon its completion.

Overview of Ordinance Provisions

The Ordinance reflects emerging practices in other cities to balance public safety and privacy concerns. Specifically, the Ordinance:

- Requires a public hearing and the approval of the City Council before the City can enter or renew an ALPR system contract
- Restricts ALPR search capabilities to only NBPD personnel who have been certified by a supervisor as having completed ALPR training requirements
- Requires all ALPR searches or data exports to be logged and subject to an annual audit
- Prevents the City from retaining ALPR data for a period greater than 30 days unless the information is relevant to an ongoing criminal or internal investigation
- Deactivates ALPR access to individuals when access is no longer necessary
- Prohibits the sale of ALPR data
- Requires the NBPD to adopt procedures for reviewing allegations of unauthorized ALPR access
- Requires an NBPD officer to visually confirm the license plate, vehicle, alert status, and relevant circumstances before taking enforcement action

- Establishes rules and regulations for sharing ALPR data upon request by an external law enforcement or criminal justice agency

- Creates monthly audits of data collection, searches, access, etc., and requires a full written report be provided to the City Council, and secondary public report demonstrating aggregate findings, substantiated violations, and corrective actions

- Prohibits ALPR vendors from retaining, accessing, processing, selling, sharing, disclosing, or analyzing collected data unless expressly required by law following the termination of a contract

Thank you for your consideration of this important measure.

Sincerely,

Jon Mitchell
Mayor

Attachment

CITY OF NEW BEDFORD

In Year Two Thousand-Twenty-Six

AN ORDINANCE

Amending Chapter 2, Administration

Be it Ordained by the City Council of the City of New Bedford as follows: -

SECTION 1. Article I of Chapter 2 of the Code of Ordinances of the City of New Bedford is hereby amended by inserting, after Section 2-12, the following:

Sec. 2-13. Automated License Plate Readers and Mass Location-Tracking Technologies.

(A) Definitions

For purposes of this section, the following words shall have the following meanings:

"Automated License Plate Reader" ("ALPR") means a camera and associated hardware or software that automatically captures or processes an image of a license plate or searchable vehicle characteristics and creates a record that may be used to identify or locate a vehicle.

The term does not include:

1. a general-purpose camera, unless automated license-plate-recognition functionality is enabled and activated;
2. a device that detects only vehicle presence, speed, weight, traffic volume, or traffic flow without retaining identifiable license plate information; or
3. a system used solely for access control, parking access, or traffic engineering that does not retain searchable license plate information for law-enforcement or investigative use.

"ALPR Data" means data collected, generated, stored, or processed through an ALPR system or Mass Location-Tracking Technology on behalf of the City. The term does not include data merely transmitted through, viewed by, or incidentally accessible to the City when the City does not possess, control, or retain the data.

"Authorized Public-Safety Purpose" means a purpose related to a criminal enforcement action or investigation, a missing or endangered person, protection of critical infrastructure or a public event, a police department internal investigation, police compliance auditing, system maintenance, or sanctioned training by the police department. Use of ALPR Data in an investigation whose primary purpose is civil immigration enforcement is not an "Authorized Public-Safety Purpose".

"Mass Location-Tracking Technology" means a system whose primary purpose or configured use is to

employ ubiquitous automated identification, correlation, or analysis to create a persistent or substantially comprehensive record of the movements of an identifiable person, device, or vehicle across multiple locations or over time.

The term does not include:

1. a camera that does not perform automated identification or persistent location tracking, including body-worn or vehicle cameras;
2. traffic-signal, traffic-engineering, or roadway-management systems that do not create person-specific or vehicle-specific travel histories;
3. City fleet management, automatic vehicle location, emergency communications, computer-aided dispatch, or employee-safety systems;
4. access-control, building-security, facility-security, port-management, or event-security systems;
5. evidence-management systems;
6. cybersecurity, network-security, or system-access logs;
7. technology deployed pursuant to a warrant, court order, or other lawful judicial process in connection with a specific investigation; or
8. technology temporarily deployed in accordance with the emergency provisions of this section.

An otherwise excluded system shall be considered Mass Location-Tracking Technology if it is subsequently configured or used to perform automated identification and create persistent or substantially comprehensive location histories.

"Material Modification" means a change that:

1. substantially expands an approved purpose of a covered system;
2. adds a substantially different category of data;
3. enables a substantially different identification, correlation, or tracking capability;
4. authorizes routine access by a substantially different category of external users; or
5. substantially increases the deployment scale.

"Material Modification" does not include:

1. maintenance or repair of system hardware or software;
2. replacement with substantially similar equipment;
3. relocation of an existing device;
4. cybersecurity, reliability, or software improvements that do not activate a materially different collection or tracking capability;
5. changes in authorized personnel consistent with an approved category of access; or
6. routine system configuration within an approved policy, appropriation, and authorized purpose.

(B) General Requirements

No City department, agency, board, commission, office, authority, or other municipal entity shall acquire, purchase, lease, license, renew, deploy, operate, or materially modify an ALPR system or Mass Location-Tracking Technology except in accordance with this section.

(C) City Council Approval After Public Hearing

The City may not enter into or renew a contract to operate an ALRP system or materially modify such system

without the approval of the City Council after a public hearing of the proposed system before the City Council subcommittee with jurisdiction over the matter.

(D) Public Safety Purpose and Privacy Assessment

Prior to the hearing, the Police Department shall prepare a Public Safety Purpose and Privacy Assessment, which shall address the following:

1. the technology and its capabilities;
2. the operational need and proposed purposes;
3. the types of information collected;
4. the anticipated number of devices and the criteria used to determine their placement;
5. the manner in which the information will be collected and used;
6. the default retention period and applicable preservation exceptions;
7. the categories of persons and entities authorized to access the information;
8. the circumstances under which information may be searched, accessed, preserved, or disclosed;
9. system architecture, cybersecurity protections, authentication, and access controls;
10. applicable constitutional, statutory, and civil-liberties considerations;
11. known accuracy limitations and the process for confirming system-generated information;
12. measures to mitigate potentially disparate impacts upon protective classes of persons;
13. safeguards intended to mitigate identified risks;
14. reasonably available alternatives; and
15. the anticipated cost to the City.

The completed assessment shall be made publicly available prior to the hearing.

(E) Device Locations

To promote public safety, the integrity of investigations, and the preservation of evidence, the Police Department shall have the sole authority to determine the location of ALPR devices and shall not be required to disclose their locations to the public in the absence of a court order. The Chief of Police may determine locations of ALPR devices without public notice.

(F) Data Governance Requirements

1. ALPR searches may be conducted only by Police Department personnel who have been certified by a supervisor as having completed the training requirements as set forth herein, and only for an Authorized Public Safety Purpose.

2. Each search or export of ALPR Data, including those conducted by another agency, shall be logged and such log shall remain subject to audit as provided herein.

3. The City shall not retain ALPR Data for a period exceeding 30 days unless the information is relevant to an open criminal or internal investigation or whose retention is otherwise required by law;

4. The Police Department shall deactivate access of any individual when such access is no longer necessary to the discharge of the individual's duties and responsibilities or upon the discovery of credible evidence that the individual has utilized the system for a purpose that is not an Authorized Public Safety Purpose;

5. The City may not sell ALPR Data;

6. Generally accepted standards of encryption, authentication, cybersecurity, access control, and

protection against unauthorized access shall apply;

7. The Police Department shall implement procedures for reviewing allegations of unauthorized access, misuse, inaccurate alerts, or security incidents; and

8. When circumstances reasonably permit, an officer shall visually confirm the license plate, vehicle, alert status, and relevant circumstances before taking enforcement action.

(G) Vendor Requirements

1. Any new or renewed agreement between the City and a vendor providing an ALPR system or Mass Location-Tracking Technology shall incorporate the applicable requirements of this section and any relevant Police Department policies promulgated hereunder.

2. The agreement shall provide that a material violation of applicable data restrictions, retention requirements, access requirements, security obligations, or data-sharing prohibitions by the vendor constitutes a material breach.

3. No vendor shall own or use ALPR Data for a purpose unrelated to the City's expressly authorized use of the system.

4. A vendor shall not sell, monetize, or commercially exploit ALPR Data.

5. Vendor personnel may access ALPR Data only to the extent reasonably necessary to provide contracted technical support, maintenance, security, or legal compliance. Such access shall be documented and subject to contractual confidentiality, security, retention, and audit requirements.

(H) External Access and Data Sharing

1. ALPR Data shall not be made available through unrestricted or open external access.

2. The Police Department may share ALPR Data upon request by an external law enforcement or criminal justice agency so long as the requesting agency has acknowledged that:

   a. The data will be used only for an Authorized Public Safety Purpose;
   b. That the data will be retained in accordance with this section; and
   c. That the data will be protected from unauthorized access or further dissemination.

3. Emergency sharing of ALPR Data shall be logged consistently with this section and reviewed by a police supervisor for compliance with this section as soon as practicable.

(I) Auditing and Compliance Review

The Police Department's Professional Standards Division shall conduct monthly reviews of the use of the system to determine compliance with this provision and any Department policies promulgated thereto.

1. Monthly audits shall examine a representative sample of:

   a. user-initiated searches;
   b. stated purposes and associated case or incident information;
   c. system alerts;
   d. data exports and external disclosures;

e. established lists or alerts such as "hot-lists";
f. user access and account status;
g. retention and destruction; and
h. any identified anomaly, complaint, or suspected unauthorized use.

2. The Department shall conduct an annual audit of the system, subject to City Council appropriation, which shall include a review of the following:

a. data collection;
b. searches and access;
c. retention, preservation, and destruction;
d. data sharing and disclosure;
e. cybersecurity and data security;
f. compliance with the Data Governance Policy;
g. compliance with this section;
h. compliance with contractual requirements;
i. training and user authorization; and
j. corrective actions taken in response to prior findings.

3. A written report of the audit shall be provided to the City Council.

4. A public audit report shall present aggregate findings, substantiated violations, and corrective actions. The Police Department may redact information protected by law or reasonably likely to compromise officer or public safety, victim or witness privacy, cybersecurity, system integrity, an active investigation, or a confidential law-enforcement method.

(J) <u>Vendor Data Disposal and Transition Requirements</u>

Upon termination, expiration, or non-renewal of an agreement involving an ALPR system or Mass Location-Tracking Technology, the Administration shall obtain written certification from the vendor establishing that:

1. The vendor has transferred to the City, in a reasonably usable format, only ALPR Data that the City is legally required or authorized to preserve, including data subject to:

a. an active evidentiary preservation requirement;
b. a criminal, civil, administrative, or internal investigation;
c. a litigation hold;
d. a warrant, court order, subpoena, or preservation request;
e. an applicable records-retention requirement; or
f. another lawful preservation obligation.

2. ALPR Data not subject to a lawful preservation requirement must be deleted or rendered permanently inaccessible in the vendor's active systems;

3. Residual backup copies must be permanently deleted or rendered permanently inaccessible through the vendor's documented backup-rotation schedule; and

4. City-owned hardware must be returned or otherwise disposed of as directed by the City.

(K) Prohibition on Vendor Retention and Secondary Use

Following the termination or expiration of an agreement, no vendor shall retain, access, process, sell, share, disclose, commercialize, analyze, or otherwise use ALPR Data except:

1. to satisfy a documented legal-preservation obligation;
2. to complete deletion through an approved backup-rotation schedule; or
3. as otherwise expressly required by law.

Any contractual provision purporting to authorize vendor ownership, sale, commercial exploitation, or unrelated secondary use of ALPR Data shall be prohibited in a new or renewed agreement to the maximum extent permitted by law.

(L) Inclusion in the Budget

The Police Department's annual budget submission shall identify each ALPR system and the amount budgeted for its use.

(M) Emergency Authority and Continuity of Operations

1. When the Chief of Police or designee reasonably determines that temporary deployment or access is necessary to address an imminent threat to life, a critical incident, a missing, abducted, or endangered person, a declared emergency, or a credible threat to critical infrastructure, the Department may temporarily deploy or access a covered technology without prior City Council approval.

2. An emergency use shall:

   a. be limited to the purpose of giving rise to the emergency;
   b. be logged consistently with this section and department policy;
   c. comply with applicable access, security, retention, and audit requirements;
   d. be subject to supervisory review; and
   e. cease when the emergency purpose ends or after 30 days, whichever occurs first, unless continued use is authorized by the City Council or governed by a warrant, court order, or other lawful authority.

3. The Chief of Police shall provide notice to the Mayor and City Council President within five business days, subject to lawful redaction and any delay reasonably necessary to protect an active investigation, public safety, or a confidential law-enforcement operation.

4. Nothing in this section shall require the interruption of an active emergency operation, investigation, prosecution, evidence-preservation obligation, or effort to locate a missing or endangered person because a contract expires, a vendor changes, or an authorization is under review.

(N) Training

Every person authorized to access an ALPR system or Mass Location-Tracking Technology must complete initial training and annual refresher training concerning:

1. authorized and prohibited uses;
2. constitutional and statutory requirements;
3. Department policy;

4. data security and confidentiality;
5. search documentation;
6. creation and maintenance of "hot-lists";
7. alert verification;
8. external disclosure restrictions; and
9. consequences of misuse.

(O) Severability

If any provision of this section or the application thereof to any person, entity, department, agency, board, commission, office, authority, technology, or circumstance is held invalid, such invalidity shall not affect the remaining provisions or applications of this section, which shall remain in full force and effect.

SECTION 2.

This ordinance shall take effect in accordance with the provisions of Chapter 43 of the Massachusetts General Laws.