

Please Note: This is a working draft containing proposed changes to this directive. The Portland Police Bureau has not yet implemented the changes. The changes can be viewed in the redline draft included in this attachment.

Submit comments using this [survey](#).

Second Universal Review: 1/15/26 – 2/14/26

0625.00 Automatic License Plate Reader Use

Refer:

- ORS 181A.250 Specific information not to be collected or maintained
- Law Enforcement Data Systems (LEDS)
- National Crime Information Center (NCIC)
- DIR 0317.40, Authorized Use of Bureau Resources
- DIR 0810.10, Bureau Contact with Members of Immigrant Communities and Individuals with Diplomatic Immunity
- DIR 1500.00, Training

Definitions:

- Automatic License Plate Reader: A device that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest.
- Automatic License Plate Reader System User: A member who accesses or operates ALPR software or a device in a Bureau vehicle, through the mobile companion application, Vigilant, Vehicle Manager, or any other current and future components of the Motorola ALPR solution.
- Bulk Tagging: A broad search that includes an inquiry for specified vehicle characteristics (e.g., year, make, model, color) and a defined location (i.e., geo-zone) and yields multiple vehicles that match any search criteria. Bulk Tagging results also include license plate Reads that do not match any plates on the Hot List.
- Hot List: License plate(s) associated with vehicles of interest from an associated law enforcement database.
- Hot Plate: License plate records that trigger alerts when a matching license plate is detected by the ALPR system.
- Reads: Data obtained by an ALPR of license plate within public view, including images of the plate and vehicle on which it was displayed, and information regarding the location of the police vehicle at the time of the ALPR data collection.

Policy:

1. This directive establishes the requirements for using Automatic License Plate Readers (ALPR) and the maintenance and sharing of data collected by ALPRs.

Please Note: This is a working draft containing proposed changes to this directive. The Portland Police Bureau has not yet implemented the changes. The changes can be viewed in the redline draft included in this attachment.

Submit comments using this [survey](#).

Second Universal Review: 1/15/26 – 2/14/26

2. ALPRs are a valuable investigative tool that is designed to capture images of license plates and the areas immediately surrounding the plates. The devices do not utilize facial recognition or other biometric technology and are not designed to deliberately capture images in areas where a reasonable expectation of privacy exists. The Bureau requires members to use the devices only for legitimate law enforcement purposes, more specifically, as its use relates to an investigation in a particular criminal or civil action.

Procedure:

1. Training Requirements and ALPR System Access.

- 1.1. Training and Certification.

- 1.1.1. ALPR System Users must be LEADS certified and complete training on the use of the ALPR system and related databases before using ALPR devices or accessing ALPR data.

- 1.1.1.1. Members shall:

- 1.1.1.1.1. Complete required ALPR training when prompted and acknowledge completion of the training in the Learning Management System;

- 1.1.1.1.2. Retain proof of their certification; and

- 1.1.1.1.3. Submit proof of their certification when requesting ALPR access.

- 1.1.1.2. If completing optional additional ALPR training, members must adhere to the procedures set forth in Directive 1500.00, Training, regarding external or third-party training documentation.

- 1.2. Access.

- 1.2.1. The Bureau shall limit member access to the ALPR system and derivative data by allowing only designated members to have routine system access.

- 1.2.1.1. Members who have an operational need for access but have not been authorized to use the ALPR system must receive Responsibility Unit (RU) Manager approval to access the system and submit a request for access to the Technology Integration Group (TIG).

- 1.2.1.2. TIG shall coordinate with Information Technology Division (ITD) to manage and execute the requests.

- 1.2.1.3. The Operations Branch shall maintain a Standard Operating Procedure that identifies the designated members and authorized reasons for adding additional System Users.

- 1.2.2. When accessing the ALPR system, members shall use the same login protocols as when accessing other law enforcement databases such as vRMS, NCIC, or LEADS. The system shall maintain a record of all database access activity.

2. Authorized and Restricted Use of ALPRs.

- 2.1. Authorized Use.

Please Note: This is a working draft containing proposed changes to this directive. The Portland Police Bureau has not yet implemented the changes. The changes can be viewed in the redline draft included in this attachment.

Submit comments using this [survey](#).

Second Universal Review: 1/15/26 – 2/14/26

- 2.1.1. Members are authorized to use ALPRs and associated databases solely for legitimate law enforcement purposes in accordance with the law. Examples include, but are not limited to the following:
 - 2.1.1.1. Locating stolen vehicles and license plates.
 - 2.1.1.2. Locating wanted, endangered, or missing persons.
 - 2.1.1.3. Canvassing a crime scene.
- 2.2. Members may use Bulk Tagging to locate vehicles they reasonably believe to be involved in a crime or to identify vehicles present in a specific geographic location at the time a crime was committed.
- 2.3. Restricted Use.
 - 2.3.1. Members shall not obtain, attempt to obtain, or convert any data obtained with an ALPR for their personal use or the unauthorized use of another person.
 - 2.3.2. Members shall not use ALPR systems or data to conduct or assist with immigration enforcement investigations or operations, unless required by law.
 - 2.3.3. Unless there is a criminal nexus, ALPR System Users shall attempt to avoid public order events or other legally protected First Amendment activity if the sole purpose is to obtain plate read intelligence. This does not preclude members from responding to a call for service where there may be incidental plate reads, or from searching for stolen vehicles and vehicles of interest in these areas.
3. Hot Plate Verification and Confirmation.
 - 3.1. A Hot Plate alert alone does not create reasonable suspicion to take police action. When an ALPR System User receives an alert indicating a Hot Plate, they shall, as soon as feasible, visually confirm that the digital image of the Hot Plate matches the Hotlist.
 - 3.2. Enter a disposition for the Hot Plate before removing the it from the Mobile Data Computer (MDC).
 - 3.3. If the system generates a valid Hot Plate, the ALPR System User shall confirm the Hot Plate by radio or documenting it in the MDC before taking any enforcement action that is based solely on Hot Plate alert, absent exigent circumstances.
4. Data Retention.
 - 4.1. The Bureau shall maintain all recorded ALPR data for a minimum of 30 days and no longer than two years. The system will automatically purge all plate reads two years after collection.
 - 4.1.1. Data must be purged once the maximum retention period has been reached unless it has become or it is reasonable to believe it will become evidence in a specific

Please Note: This is a working draft containing proposed changes to this directive. The Portland Police Bureau has not yet implemented the changes. The changes can be viewed in the redline draft included in this attachment.

Submit comments using this [survey](#).

Second Universal Review: 1/15/26 – 2/14/26

criminal or civil action. In such circumstances, a System Coordinator shall download the applicable data from the server onto a portable drive. The download data is subject to the same logging, handling, and chain of custody requirements as other evidence.

- 4.2. All downloaded ALPR data located on an ALPR System User’s laptop and server shall only be accessible through a login and password-protected system capable of documenting who accesses the information by identity, date, and time.
- 4.3. Authorized users are permitted to access the data only when there is a reasonable belief that the data relates to an investigation in a specific criminal or civil action.
5. Data Requests and Sharing.
 - 5.1. Notwithstanding any other provision of law, all electronic images or data gathered by ALPRs are for the exclusive use of law enforcement in the discharge of duties and are not to be made open to the public.
 - 5.1.1. These guidelines should not be interpreted to limit the use of the electronic images or data for legitimate purposes by prosecutors or others legally permitted to receive evidence under the law.
 - 5.2. Records Division Responsibilities.
 - 5.2.1. The Records Division (“Records”) shall manage all public records requests, coordinating with TIG, as needed.
 - 5.2.2. Records shall handle requests for lists of suspect vehicles in the database on a plate by plate basis after consulting with the investigating officer, the City Attorney’s Office, and the Public Information Officer.
 - 5.2.3. Records will charge the requesting party the actual cost of providing the record(s). Requests for stolen vehicle lists will be directed to LEDS.
 - 5.3. Technology Integration Group Responsibilities.
 - 5.3.1. TIG shall manage all requests for access to the ALPR system that are made through the system.
6. System Maintenance and Technical Support.
 - 6.1. ITD is responsible for ALPR system maintenance; however, the Program Manager shall coordinate with ITD to perform installs and software updates, provide technical assistance, and respond to system outages.
 - 6.2. If an ALPR System User discovers that a device is damaged or the member needs technical support, they shall contact their supervisor as soon as feasible.
 - 6.2.1. Supervisors shall:

Please Note: This is a working draft containing proposed changes to this directive. The Portland Police Bureau has not yet implemented the changes. The changes can be viewed in the redline draft included in this attachment.

Submit comments using this [survey](#).

Second Universal Review: 1/15/26 – 2/14/26

- 6.2.1.1. Report damage to the Program Manager as soon as feasible; and
- 6.2.1.2. Refer ALPR System Users in need of technical support to the Program Manager if they are unable to resolve the technical issue at the RU level.

7. Program Manager Responsibilities.

7.1. The Bureau shall designate a TIG supervisor to serve as the Program Manager.

7.2. The Program Manager shall:

- 7.2.1. Manage the Bureau-wide ALPR program;
- 7.2.2. Produce an annual report that includes; the number of plate reads obtained; the number of stolen vehicles recovered; notable case results; and any known misuse of the system.
- 7.2.3. Oversee and administer the operational aspects of the ALPR program, including the storage and management of all ALPR data systems and databases. This is to be done with the support of ITD;
- 7.2.4. Ensure only authorized RU (or designated) personnel have access the ALPR system;
- 7.2.5. Ensure ALPR System Users are appropriately trained and that they complete training before using the system;
- 7.2.6. Ensure System Users receive ongoing training when necessary;
- 7.2.7. Document all training;
- 7.2.8. Authorize any requests for ALPR use or data access; and
- 7.2.9. Ensure all ALPR operation and access to ALPR collected data shall be for official agency purposes only.

8. Information Technology Division Responsibilities.

8.1. The ITD Manager (or a designee) shall:

- 8.1.1. Set retention schedules;
- 8.1.2. Assist the Program Manager with maintaining the system in conjunction with the vendor.
- 8.1.3. Maintain the server systems and MDC used for the ALPR system.
- 8.1.4. Provide technical support for System Users using the ALPR server and in-car systems during regular business hours: Monday through Friday only.

445.00 AUTOMATIC LICENSE PLATE READER (ALPR)

0625.00 Automatic License Plate Reader Use

Refer:

- ~~LEDS~~
- ~~NCIC~~
- ~~PPDS~~

1. STATEMENT OF PURPOSE

- ~~1.1. This policy is established to ensure the ORS 181A.250 Specific information not to be collected or maintained~~
- Law Enforcement Data Systems (LEDS)
- National Crime Information Center (NCIC)

-
- DIR 0317.40, Authorized Use of Bureau Resources
 - DIR 0810.10, Bureau Contact with Members of Immigrant Communities and Individuals with Diplomatic Immunity
 - DIR 1500.00, Training

Definitions:

- Automatic License Plate Reader (ALPR): A device that uses cameras and computer technology to compare digital images of license plates to lists of known plates of interest.
- Automatic License Plate Reader System User: A member who accesses or operates ALPR software or a device in a Bureau vehicle, through the mobile companion application, Vigilant, Vehicle Manager, or any other current and future components of the Motorola ALPR solution.
- Bulk Tagging: A broad search that includes an inquiry for specified vehicle characteristics (e.g., year, make, model, color) and a defined location (i.e., geo-zone) and yields multiple vehicles that match any search criteria. Bulk Tagging results also include license plate Reads that do not match any plates on the Hot List.
- Hot List: License plate(s) associated with vehicles of interest from an associated law enforcement database.
- Hot Plate: License plate records that trigger alerts when a matching license plate is detected by the ALPR system.
- Reads: Data obtained by an ALPR of license plate within public view, including images of the plate and vehicle on which it was displayed, and information regarding the location of the police vehicle at the time of the ALPR data collection.

Policy:

1. This directive establishes the requirements for using Automatic License Plate Readers (ALPR) and the maintenance and sharing of data collected by ALPRs.

~~1.2. ALPRs are a valuable investigative tool that is used by~~ designed to capture images of license plates and the areas immediately surrounding the plates. The devices do not utilize facial recognition or other biometric technology and are not designed to deliberately capture images in areas where a reasonable expectation of privacy exists. The Bureau requires members ~~in a responsible and professional manner in accordance with all applicable laws and administrative rules~~ to use the devices only for legitimate law enforcement purposes, more specifically, as its use relates to an investigation in a particular criminal or civil action.

2. DIRECTIVE SPECIFIC DEFINITIONS

2.1. No definitions.

3. POLICY

3.1. Automatic license Plate Reader (ALPR) equipped cars**Procedure:**

1. Training Requirements and associated ALPR System Access.

1.1. Training and Certification.

1.1.1. ALPR System Users must be LEADS certified and complete training on the use of the ALPR system and related databases ~~are~~ before using ALPR devices or accessing ALPR data.

1.1.1.1. Members shall:

1.1.1.1.1. Complete required ALPR training when prompted and acknowledge completion of the training in the Learning Management System;

1.1.1.1.2. Retain proof of their certification; and

1.1.1.1.3. Submit proof of their certification when requesting ALPR access.

1.1.1.2. If completing optional additional ALPR training, members must adhere to ~~be used~~ the procedures set forth in Directive 1500.00, Training, regarding external or third-party training documentation.

1.2. Access.

1.2.1. The Bureau shall limit member access to the ALPR system and derivative data by allowing only designated members to have routine system access.

1.2.1.1. Members who have an operational need for legitimate law enforcement purposes ~~in accordance~~ access but have not been authorized to use the ALPR system must receive Responsibility Unit (RU) Manager approval to access the system and submit a request for access to the Technology Integration Group (TIG).

~~1.1.1.1.2.1.2.~~ TIG shall coordinate with state and federal law Information Technology Division (ITD) to manage and execute the requests.

1.2.1.3. ~~3.2. Members will~~ The Operations Branch shall maintain a Standard Operating Procedure that identifies the designated members and authorized reasons for adding additional System Users.

~~When accessing the ALPR system, members shall use the same login protocols as when accessing other law enforcement databases such as PPDSvRMS, NCIC, or LEDS when accessing the ALPR database.~~

~~1.1.2.1.2.2. 3.3. Usage of the ALPR databases will be regulated by requiring members to log into the system. A. The system shall maintain a record of all database activity will be recorded and maintained in accordance with the procedures outlined in this policy access activity.~~

~~3.4. ALPR is an investigative tool only, therefore all members will verify all "hits" prior to taking enforcement action to ensure the information is not expired or outdated.~~

~~4. PROCEDURE~~

~~4.1. Training Requirements~~

~~4.1.1. ALPR Operators must be LEDS certified and properly trained on the ALPR system and related databases prior to using ALPR equipment or accessing ALPR data.~~

~~4.2. Prohibited Use~~

~~4.2.1.~~

2. Authorized and Restricted Use of ALPRs.

2.1. Authorized Use.

~~1.1.3.2.1.1. Members are prohibited from using, or authorizing the authorized to use, of ALPR equipment or database records ALPRs and associated databases solely for non-legitimate law enforcement purposes, in accordance with the law. Examples include, but are not limited to the following:~~

~~2.1.1.1. 4.2.2. Locating stolen vehicles and license plates.~~

~~2.1.1.2. Locating wanted, endangered, or missing persons.~~

~~2.1.1.3. Canvassing a crime scene.~~

2.2. Members may use Bulk Tagging to locate vehicles they reasonably believe to be involved in a crime or to identify vehicles present in a specific geographic location at the time a crime was committed.

2.3. Restricted Use.

2.3.1. Members shall not obtain, attempt to obtain, or convert any data obtained with an ALPR for their personal use or the unauthorized use of another person.

2.3.2. Members shall not use ALPR systems or data to conduct or assist with immigration enforcement investigations or operations, unless required by law.

~~1.1.4.2.3.3. Unless there is a criminal nexus, ALPR operators will~~System Users shall attempt to avoid public gatherings such as political rallies, public demonstrations and religious gatherings; order events or other legally protected First Amendment activity if the sole purpose is to obtain plate read intelligence. This does not preclude members from responding to a call for service where there may be

incidental plate reads, or from searching for stolen vehicles and vehicles of interest in these areas.

~~4.3.~~

3. Hot Plate Verification and Confirmation.

3.1. A Hot Plate alert alone does not create reasonable suspicion to take police action. When an ALPR System User receives an alert indicating a Hot Plate, they shall, as soon as feasible, visually confirm that the digital image of the Hot Plate matches the Hotlist.

3.2. Enter a disposition for the Hot Plate before removing the it from the Mobile Data Collection and Computer (MDC).

3.3. If the system generates a valid Hot Plate, the ALPR System User shall confirm the Hot Plate by radio or documenting it in the MDC before taking any enforcement action that is based solely on Hot Plate alert, absent exigent circumstances.

2.4. Data Retention.

~~2.1.4.1.~~ 4.3.1. All ALPR data ~~The Bureau shall maintain all~~ recorded ~~should be maintained~~ ALPR data for a minimum of 30 days and no longer than ~~four~~ two years. ~~All plate reads~~ The system will ~~be~~ automatically ~~purged~~ purge all plate reads ~~two~~ years after collection.

~~2.1.1.4.1.1.~~ 4.3.2. Data must be purged once the maximum retention period has been reached unless it has become or it is reasonable to believe it will become evidence in a specific criminal or civil action. In such circumstances, a System Coordinator shall download the applicable data ~~will be downloaded~~ from the server ~~by a system coordinator~~ onto a ~~CD or other~~ portable technology drive. The download data ~~will be~~ is subject to the same logging, handling, and chain of custody requirements as other evidence.

~~4.3.3.~~

~~2.2.4.2.~~ All ALPR data ~~downloaded to the operator~~ ALPR data located on an ALPR System User's laptop and server ~~must~~ shall only be accessible ~~only~~ through a login ~~and~~ password ~~accessible-protected~~ system capable of documenting who accesses the information by identity, date, and time.

~~4.3.4. Persons approved to access ALPR data~~

~~2.3.4.3.~~ Authorized users are permitted to access the data only when there is a reasonable belief that the data relates to an investigation in a specific criminal or civil action.

~~4.3.5.~~

5. Data Requests and Sharing.

~~2.4.5.1.~~ Notwithstanding any other provision of law, all electronic images or data gathered by Automated License Plate Readers ~~ALPRs~~ are for the exclusive use of law enforcement in the discharge of duties and are not to be made open to the public.

~~2.4.1.5.1.1.~~ 4.3.6. These guidelines should not be interpreted to limit the use of the electronic images or data for legitimate purposes by prosecutors or others legally permitted to receive evidence under the law.

4.4. Information Requests

~~4.4.1. All information requests will be handled through the~~

5.2. Records Division- Responsibilities.

~~2.4.2.5.2.1. The Records Division will forward the request to the System Administrator who will provide the information in accordance with (“Records”) shall manage all public records request case law requests, coordinating with TIG, as needed.~~

~~2.4.3.1.1.1. 4.4.2. The Records Division will charge the requesting party the actual cost of providing the information. Records shall handle requests. Requests for stolen vehicle lists will be directed to LEADS.~~

~~2.4.4.5.2.2. 4.4.3. Requests for lists of suspect vehicles in the database will be handled on a plate by plate basis; after consulting with the investigating officer, the City Attorney/Attorney’s Office, and the Public Information Officer.~~

~~5.2.3. Records will charge the requesting party the actual cost of providing the record(s). Requests for stolen vehicle lists will be directed to LEADS.~~

4.5. Maintenance

~~4.5.1. Any damage will be reported immediately to the System Administrator. Technical questions concerning the ALPR will be directed to the System Administrator. Members will not directly contact the vendors(s). All vendor(s) contact will occur through the System Administrator or Information Technology Division.~~

4.6. System Administrator

2.5.5.3. Technology Integration Group Responsibilities.

~~4.6.1. A supervisor will be designated as the System Administrator.~~

~~4.6.2. The System Administrator will be responsible for the Bureau wide management of the ALPR program including the designation of a system coordinator for each RU that has an ALPR unit assigned.~~

~~5.3.1. 4.6.3. The System Administrator will produce TIG shall manage all requests for access to the ALPR system that are made through the system.~~

6. System Maintenance and Technical Support.

~~6.1. ITD is responsible for ALPR system maintenance; however, the Program Manager shall coordinate with ITD to perform installs and software updates, provide technical assistance, and respond to system outages.~~

~~6.2. If an ALPR System User discovers that a device is damaged or the member needs technical support, they shall contact their supervisor as soon as feasible.~~

~~6.2.1. Supervisors shall:~~

~~6.2.1.1. Report damage to the Program Manager as soon as feasible; and~~

~~6.2.1.2. Refer ALPR System Users in need of technical support to the Program Manager if they are unable to resolve the technical issue at the RU level.~~

7. Program Manager Responsibilities.

~~7.1. The Bureau shall designate a TIG supervisor to serve as the Program Manager.~~

~~7.2. The Program Manager shall:~~

7.2.1. Manage the Bureau-wide ALPR program;

~~2.5.1.7.2.2.~~ Produce an annual report that includes; the number of plate reads obtained; the number of stolen vehicles recovered; notable case results; and any known misuse of the system.

~~4.7. System Coordinator Responsibilities~~

~~4.7.1. System coordinators are responsible for the following:~~

~~2.5.2.7.2.3.~~ 4.7.1.1. Overseeing and administering~~Oversee and administer the operational aspects of~~ the ALPR program, including the storage and management of all ALPR data systems and databases. This is to be done with the support of ~~Information Technology Division (ITD).~~ITD;

~~2.5.3.7.2.4.~~ 4.7.1.2. Ensuring the proper selection of the~~Ensure only authorized RU (or designated) personnel approved to operate~~have access the ALPR system.;

~~2.5.4.7.2.5.~~ 4.7.1.3. Ensuring appropriate~~Ensure ALPR System Users are appropriately trained and that they complete training of operators and that training is completed prior to an operator~~before using the system.;

~~4.7.1.4. Ensuring all training is documented.~~

~~2.5.5.7.2.6.~~ 4.7.1.5. Ensuring~~Ensure System Users receive~~ ongoing training ~~is provided as deemed~~when necessary.;

~~7.2.7.~~ 4.7.1.6. Authorizing~~Document all training;~~

~~2.5.6.7.2.8.~~ Authorize any requests for ALPR use or data access.;

~~2.5.7.7.2.9.~~ 4.7.1.7. Ensuring~~Ensure~~ all ALPR operation and access to ALPR collected data shall be for official agency purposes only.

~~4.8. ITD Responsibilities~~

~~4.8.1. The~~

~~8. Information Technology Division~~ (Responsibilities.

~~2.6.8.1.~~ The ITD) manager ~~Manager~~ (or ~~their~~a designee ~~will be responsible for the following) shall:~~

~~4.8.1.1. Maintaining the ALPR database to ensure retention guidelines are followed.~~

~~8.1.1.~~ 4.8.1.2. Assisting the system administrator~~Set retention schedules;~~

~~2.6.1.8.1.2.~~ Assist the Program Manager with maintaining the system in conjunction with the vendor.

~~2.6.2.8.1.3.~~ 4.8.1.3. Maintaining~~Maintain~~ the server systems and MDC used for the ALPR system.

~~4.8.1.4. Making the~~Provide technical ~~connections to other databases including LEADS as needed for stolen plate downloads or data sharing with other agencies.~~

~~2.6.3.8.1.4.~~ 4.8.1.5. ITD will support ~~for System Users using~~ the ALPR server and in-car systems during regular business hours: Monday through Friday only.

#1

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Friday, August 01, 2025 12:51:38 PM
Last Modified: Friday, August 01, 2025 12:53:07 PM
Time Spent: 00:01:28

Page 1

Q1

Please provide feedback for this directive

This tool should be invaluable in helping convict so many dangerous criminals!

Q2

Contact Information (optional - your name will be visible on PPB's website)

Name **Tim Larson**

#2

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Friday, August 15, 2025 9:40:00 AM
Last Modified: Friday, August 15, 2025 9:42:07 AM
Time Spent: 00:02:07

Page 1

Q1

Please provide feedback for this directive

Re 4.2.2

'4.2.2. Unless there is a criminal nexus, ALPR operators will attempt to avoid public gatherings such as political rallies, public demonstrations and religious gatherings; if the sole purpose is to obtain plate read intelligence. '

Why, pubic gathering are no different than public use of a vehicle. If the intent is to identify non legal activity related to a plate number it should always be used.

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#3

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Tuesday, August 19, 2025 9:42:18 PM
Last Modified: Tuesday, August 19, 2025 9:45:20 PM
Time Spent: : 00:03:02

Page 1

Q1

Please provide feedback for this directive

I am concerned that information in this database could be used by federal agencies for purposes that go beyond the intention of PPB. What safety mechanisms are in place to prevent this from happening, if any?
Also, the intention to not use this around public demonstrations seems more a suggestion than a prohibition. What protocols are in place if this is indeed happening, to prevent in future?

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#4

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Saturday, August 30, 2025 10:17:45 AM
Last Modified: Saturday, August 30, 2025 10:20:42 AM
Time Spent: 00:02:57

Page 1

Q1

Please provide feedback for this directive

Re: 445.00 AUTOMATIC LICENSE PLATE READER (ALPR) Policy

First Universal Review: 08/01/25 - 08/31/25

I am an independent researcher living in North Portland who has investigated use of surveillance and algorithmic technology systems by Portland government for several years. The goal of this work is to provide evidence-based research and analysis to help inform and improve government policy and policy implementation related to City government use of these highly complex technical systems and the data about people in Portland flowing through these systems. I welcome the opportunity to provide comment regarding Portland Police Bureau's 445.00 Automatic License Plate Reader (ALPR) policy as part of its Police Directive First Universal Review process. In the following comments I point to specific areas mentioned in the policy that could benefit from additional detail and guidance. I also highlight existing, applicable Portland policy and documentation related to use of ALPRs.

Now is a good time for a thorough review and possible amendment of the 445.00 ALPR policy to ensure it addresses the complexities of current technological advancements, data connections, system interoperability and data sharing practices associated with ALPR use.

Although there has been very little information made public regarding the ALPR systems used by PPB, a 2014 City of Portland Legislative Report stated, "Portland Police Bureau is the largest user of Automatic License Plate Reader (ALPR) technology in Oregon." Media reports have stated that PPB's plate readers track and identify anywhere from 8,000 to 128,000 license plates each day, and that sensitive information reflecting the owners of vehicles associated with those plates is shared with a variety of other organizations and systems.

It is important to note that the 445.00 ALPR policy under review is the same exact policy established by a 2013 executive order, when ALPRs and related data technologies, data connections and sharing practices, data related agreements and processes, and ownership of vendors supplying PPB's ALPR systems and services may have been different. Understanding these details will help ensure that policy remains relevant and effective amid current realities.

Today's connected tech is not static and rarely remains as it was when it was originally purchased. New or supplemental system capabilities, features and data connections can be added or enabled readily through software updates and operations that may not require procurement approval. Such behind-the-scenes alterations can alter or expand capabilities in meaningful ways.

Simply approving the existing policy may not fulfill Portland's oft-stated goals for transparency and accountability when it comes to protecting privacy and limiting negative impacts of surveillance in relation to technology use by the City. This policy review process should be conducted in conjunction with Portland's elected officials representing the people of Portland who are affected by use of ALPRs and ALPR data use and sharing, as well as in conjunction with people living here.

A Privacy Impact Assessment and/or Surveillance Impact Assessment

As part of the review process, policymakers could consider conducting a Privacy Impact Assessment and/or Surveillance Impact Assessment of PPB's ALPR system. Despite the fact that ALPRs have been used by PPB for more than a decade, no PIA has been conducted. A 2021 PIA of a Portland Bureau of Transportation pilot of an ALPR system for parking enforcement found medium- and high-level risks related to Privacy Harms, Equity, Disparate Community Impact, The City's Political, Reputation and Image and City Business, Quality and Infrastructure. The PIA recommended minimization of ALPR related data collection. Adequate funding and resources for Smart City PDX is necessary to ensure appropriate transparency and accountability for Portland's use of tech affecting privacy such as surveillance tech systems.

PPB and Portland City Council might consider further clarification and refinement of the 445.00 ALPR policy in relation to the following:

ALPR Data Access and Data Sharing Protocols and Connectivity

0445.00 Directive Feedback (1UR)

- The policy under review states, “Members will use the same protocols as accessing other law enforcement databases such as PPDS, NCIC, or LEDS when accessing the ALPR database.” It also states The Information Technology Division (ITD) makes “the technical connections to other databases including LEDS as needed for stolen plate downloads or data sharing with other agencies.”
- Information about these protocols for and connectivity to internal and external or third-party data systems including in relation to intergovernmental data sharing with local, state, and federal law enforcement and formal or informal collective law enforcement data and information-sharing networks are not explained in the policy and have not been made public. Additional detail regarding these protocols, connectivity between PPB’s ALPR systems and other databases or systems including the LEDS (Law Enforcement Data System), NCIC (National Crime Information Center) system, and PPDS (Portland Police Data System) is necessary to understand the full extent of ALPR collection, use, sharing and access.
- Additional clarification regarding involvement of other Portland Bureaus in technical ALPR operations and implementation such as Bureau of Technology Services and Bureau of Emergency Communications would also be helpful.

Data Collection and Retention

- The policy under review states that all ALPR data recorded should be “automatically purged four years after collection...unless it has become or it is reasonable to believe it will become evidence in a specific criminal or civil action.”
- To better understand the implementation and effectiveness of this data retention policy, it would be helpful for City Council and the public to know whether any PPB ALPR data has ever been purged and how, whether any PPB ALPR data has been stored after four years and under what circumstances, and whether and how that PPB ALPR data has been used, shared or accessed.

ALPR Purpose and Purpose Limitations

- The 445.00 ALPR policy states, “Unless there is a criminal nexus, ALPR operators will attempt to avoid public gatherings such as political rallies, public demonstrations and religious gatherings; if the sole purpose is to obtain plate read intelligence. This does not preclude members from responding to a call for service where there may be incidental plate reads, or from searching for stolen vehicles and vehicles of interest in these areas.”
- Further information regarding PPB’s ALPR purposes and purpose limitations including definitions and guidance regarding ALPR use in situations involving a “criminal nexus” could be included in the policy, or at least clarified for improved understanding during policy review.

ALPR Use and Misuse in Annual ALPR Reports

- The policy in review states that the “System Administrator will produce an annual report that includes; the number of plate reads obtained; the number of stolen vehicles recovered; notable case results; and any known misuse of the system.” In order to understand more about actual use and misuse of the ALPR system, it would be helpful for City Council and the public to access these reports. At the very least, guidance regarding publication and access to these reports should be clarified, including whether they might be included in the City’s forthcoming surveillance technology inventory and registry.

ALPR Hardware, Software and System Makers and Service Providers

- As noted above, capabilities of today’s connected tech can be altered or expanded with the flick of a proverbial switch. In order to understand the capabilities of PPB’s ALPR devices, systems, as well as data use, sharing, and impacts of these systems, more information regarding the actual makes and models of PPB’s ALPR software, hardware, data servers, in-car systems and other related devices or systems is necessary. Some of this information may have been provided in response to the City’s surveillance technology inventory that is underway in relation to Portland’s 2023 Surveillance Resolution.

Existing Relevant Portland Policy

Two existing Portland policies established recently -- Portland’s 2019 Privacy Resolution and its 2023 Surveillance Resolution -- are not referenced in the 445.00 ALPR policy but are applicable to ALPR technologies and data use.

Portland’s 2023 Surveillance Resolution

- Portland’s 2023 Surveillance Resolution called for the Bureau of Planning and Sustainability Smart City PDX and the Office of Equity and Human Rights to coordinate with the Bureau of Technology Services to develop policies and procedures required for

0445.00 Directive Feedback (1UR)

implementing Privacy Impact Assessments (PIA) when procuring or planning to use Surveillance Technologies. It appears as though no PIA of the ALPR hardware, software, or systems used by PPB has ever been conducted.

- The resolution called for an inventory of surveillance technologies used by the City. The inventory should include information related to ALPR hardware, software, and systems used by PPB.
- The Surveillance Resolution also called for the Bureau of Planning and Sustainability, Smart City PDX and the Office of Equity and Human Rights to design accountability and oversight strategies and procedures for the use and acquisition of surveillance technologies in public and equitable processes.

Portland's 2019 Privacy Resolution

- Portland's 2019 Privacy Resolution stated a commitment by the City Council to use of the City's Privacy and Information Protection Principles when considering policies and projects that require the collection, use, management and disposal of Data and Information -- such as use of ALPRs and ALPR-related data.
- Portland's Privacy Principles require that City use, management and collection of information be "described clearly, accurately, and shared in an accessible way" and that information regarding creation, contribution and access to data be "clearly documented and communicated to all people who entrust the City with their Data and Information."
- The Privacy Resolution called for stewardship, security and protection of data including in relation to its storage, processing, retention and disposition throughout the full lifecycle of the system in use.

Other Relevant Existing Documentation

2022 PPB Audit Status Report

- Portland's Police Bureau 2022 Audit Status Report states, "The Bureau should adopt a technology directive that includes Council authorization of surveillance technology, advice from a privacy commission, and requirements for policies and reporting." ALPRs have been used by PPB for more than a decade; however, documentation related to Council authorization of this form of surveillance technology is not readily available. In addition, it is unclear whether any privacy commission has been formed.

Automated Decision Systems and AI Related Policy

- Portland's Surveillance Resolution calls for the Bureau of Planning and Sustainability Smart City PDX and the Office of Equity and Human Rights to "conduct an initial assessment of the impacts of Automated Decision Systems on Portlanders, visitors, and City staff to identify additional privacy and information protection policies." In part because there is a lack of publicly-available information regarding the actual ALPR hardware, software and systems currently owned by or in use by PPB, it is not known whether they incorporate ADS or AI.
- ADS or AI related features and capabilities in ALPR systems or in other systems connected to PPB's ALPR systems (such as facial or biometric recognition systems, or algorithmic and AI-based predictive systems) may create additional privacy and surveillance related impacts necessary to consider.

Portland Bureau of Transportation ALPR Pilot Privacy Impact Assessment

- Smart City PDX conducted a PIA of a Portland Bureau of Transportation pilot of an ALPR system for use in one vehicle for parking permit enforcement.
- According to that 2021 PIA, Smart City PDX found medium and high-level risks related to Privacy Harms, Equity, Disparate Community Impact, The City's Political, Reputation and Image and City Business, Quality and Infrastructure.
- The PIA recommended minimization of ALPR related data collection. As mentioned in that PIA, the assessment was deemed incomplete because there was a lack of documentation connected to the system and maker of the system, related third parties, and their privacy and data policies.

I am grateful for your consideration of these comments in reviewing the 445.00 Automatic License Plate Reader (ALPR) policy. The research and writing presented in these comments was conducted in my own personal time and the content of these comments is in no way connected to my employer.

Thank you,
Kate Kave

Kate Kaye

Independent researcher of algorithmic and surveillance tech and data use

North Portland resident

RedTailMedia.org

Q2

Contact Information (optional - your name will be visible on PPB's website)

Name

Kate Kaye, Kate@redtailmedia.org

#5

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Saturday, August 30, 2025 11:00:00 AM
Last Modified: Saturday, August 30, 2025 11:07:28 AM
Time Spent: 00:07:27

Page 1

Q1

Please provide feedback for this directive

I would like the policy to specifically mandate, if it does not already do so, that all data processing and retention must be done by city employees and city infrastructure, and not done through outsourcing to a 3rd party such as Flock. The security records of such companies are beyond abysmal, and constitute a significant threat to the privacy of city residents.

Q2

Contact Information (optional - your name will be visible on PPB's website)

Name **20-year resident of SE Portland**

#6

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Saturday, August 30, 2025 10:09:14 PM
Last Modified: Saturday, August 30, 2025 10:10:31 PM
Time Spent: 00:01:17

Page 1

Q1

Please provide feedback for this directive

This language inadequately addresses basic privacy and data security issues that are fundamental to responsible policymaking.

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#7

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Sunday, August 31, 2025 5:22:50 PM
Last Modified: Sunday, August 31, 2025 5:24:52 PM
Time Spent: 00:02:02

Page 1

Q1

Please provide feedback for this directive

Absolutely opposed to this, for despite promises and contractual obligations, the data from ALPR systems always finds its way to ICE. You can't guarantee someone greedy won't accept the absurdly high rewards DHS is giving to its quisling collaborators.

Q2

Contact Information (optional - your name will be visible on PPB's website)

Name **J. E. Bartley**
