TECHNOLOGY

DECEMBER 2024

# Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

**Acknowledgement**

We would like to thank the Ontario Provincial Police for reviewing an earlier version of these guidelines, first published in 2017, and providing helpful comments. While updating this guidance, the IPC consulted several experts, including members of other police services and academia. We would like to thank these individuals for their feedback.

# CONTENTS

BACKGROUND ..... 1

INTRODUCTION ..... 1

DEFINITIONS ..... 2

WHAT IS ALPR TECHNOLOGY? ..... 3

- Types of ALPR technology ..... 3

PERSONAL INFORMATION ..... 4

PRIVACY IMPLICATIONS OF ALPR SYSTEMS ..... 4

SYSTEM CONFIGURATION ..... 5

CONDUCT A PRIVACY IMPACT ASSESSMENT (PIA) ..... 6

- Additional considerations for fixed ALPR ..... 6

CONSULT THE IPC ..... 7

CONDUCT A PILOT ..... 7

POLICIES AND PROCEDURES ..... 8

- Authority, scope and purpose of the Program ..... 8
- Collection ..... 8
- Notice ..... 9
- Transparency ..... 10
- Use ..... 10
- The scope of the hotlists ..... 11
- Manual entries ..... 11
- Manual searches ..... 12
- Managing hit and non-hit information ..... 12
- Secondary uses of ALPR hit information ..... 13
- Internal access to the ALPR system ..... 13
- Disclosure ..... 13
- Retention ..... 14
- Accuracy ..... 14
- Security ..... 14
- Reviews and audits ..... 15
- Training ..... 16
- Complaint and redress mechanisms ..... 16
- Access to information requests ..... 17

CONCLUSION ..... 17

APPENDIX A: CATEGORIES OF PLATES GATHERED FROM THE MINISTRY OF TRANSPORATION (MTO) AND THE CANADIAN POLICE INFORMATION CENTRE (CPIC) ..... 18

APPENDIX B: CATEGORIES OF MANUAL PLATE ENTRIES ..... 19

APPENDIX C: SUMMARY OF KEY RECOMMENDATIONS ..... 20

## BACKGROUND

The Information and Privacy Commissioner of Ontario (IPC) first published guidance on police use of automated licence plate recognition (ALPR) technology in 2017. Since then, new circumstances and uses of ALPR have revealed additional issues and factors to consider. Updates have been made to this guidance for clarity, consistency, and emphasis of key considerations.

In recent years, police use of mobile ALPR systems has grown significantly across Ontario, spurred on by government investments and police uptake of the technology. In 2022, the Government of Ontario eliminated the requirement for licence plate validation stickers and associated renewal fees on passenger vehicles, light-duty trucks, motorcycles, and mopeds.[1] To replace physical licence plate stickers, improve public safety and strengthen roadside enforcement efforts, the government introduced a one-time ALPR grant for police to adopt the technology.

While some Ontario police services were already using mobile ALPR systems prior to 2022, the grant allowed police to acquire newer, more sophisticated ALPR units with better cameras, software, and interoperability. In some cases, police services were able to equip every vehicle in their fleet with the technology. The grant also allowed police services that did not previously have the technology to acquire and implement it. As a result, ALPR systems are now being deployed across Ontario in significant numbers.

In Ontario, ALPR is generally deployed in or on police vehicles. However, ALPR systems can also be installed at fixed locations, such as telephone poles or highway overpasses. Further, ALPR software can be integrated into other police technologies, such as in-car camera systems (ICCS) and closed-circuit television systems (CCTV) to scan licence plates, expanding the capabilities of these systems and technologies.

Given the significant additional privacy and surveillance risks associated with fixed ALPR systems, the IPC has updated the guidelines to address these new risks.

## INTRODUCTION

ALPR systems can be configured to operate in either mobile or stationary (also known as fixed ALPR) environments. ALPR technology can quickly capture and match large volumes of licence plate numbers to lists of plates stored in a database. ALPR components work together, such as a camera, computer, and database, to form an ALPR system.[2] Police services in Ontario are using ALPR systems to match licence plates captured in real-time on roadways to lists of plates of interest, such as stolen and expired plates, plates registered to suspended drivers, and plates associated with missing persons or Amber Alerts where a vehicle is involved.

ALPR systems also collect other personal information when they scan a licence plate, including the date, time, and geolocation of the vehicle. As a result, these systems have the potential to be used to track individuals' locations over time and increase the risk of surveillance and profiling.

Left unchecked, the use of ALPR systems raises significant privacy concerns. While public safety is important, police use of ALPR systems must comply with Ontario's public sector privacy legislation

1 Government of Ontario February 2022 news release, **Ontario Eliminating Licence Plate Renewal Fees and Stickers**.
2 ALPR systems are also known as mobile licence plate recognition systems and automatic number plate recognition systems.

and respect the public's reasonable expectation of privacy and other fundamental rights and liberties. Proper policies, procedures and technical controls are critical to protecting privacy, particularly considering that most drivers whose vehicles are subject to ALPR systems are simply going about their everyday activities.

The IPC oversees compliance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), which applies to municipal police, and the *Freedom of Information and Protection of Privacy Act* (FIPPA), which applies to the Ontario Provincial Police (OPP).[3]

This document outlines the key obligations of police services under MFIPPA and FIPPA in their use of ALPR systems. It provides guidance, including best practices, on using these systems in a privacy-protective manner. It addresses and applies to the police use of mobile and fixed ALPR systems for specific public safety purposes. In particular, this guidance applies to the use of ALPR systems to assist officers with immediate roadside enforcement activity by alerting an officer of a particular licence plate. It does not cover the use of ALPR systems for traffic management, road tolls, parking enforcement or other investigative purposes, nor does it cover the integration of ALPR with other technologies. A different set of privacy issues and mitigation approaches may need to be considered in those other contexts. Also, other legal obligations and limitations beyond those set out in MFIPPA and FIPPA may apply to police ALPR systems and should be considered.

## DEFINITIONS

- **Automated licence plate recognition (ALPR)** is a technology that includes a camera, a computer and a database. These components work together to form an "ALPR system." When installed on a vehicle or stationary object, ALPR systems are used to identify vehicles by matching licence plate numbers to lists of plates stored in a database.
- **Hit** refers to a scanned licence plate that appears to match a plate on a hotlist.
- **Hit information** is information associated with a hit that is captured by the ALPR system and includes plate images, date, time and geolocation.
- **Hotlist** is a list of licence plates that police or affiliated institutions, such as the Ministry of Transportation (MTO), have identified as those for which police should be on the lookout (a type of watch list). Police services generally receive hotlists, updated daily from MTO and the Canadian Police Information Centre (CPIC), to which they can manually add plate numbers in defined circumstances. The hotlists are stored in the ALPR database and copied to a computer in a police vehicle. See Appendix A and B for more information about hotlists.
- **Non-hit** refers to a scanned licence plate that does not match a plate on a hotlist, or where a match is inaccurate.
- **Non-hit information** is information associated with a non-hit that is captured by the ALPR system and may include information such as plate images, date, time and geolocation.
- **Police service** refers to a municipal police service, a municipal police service board and the OPP.[4]

3 While the OPP is not an institution under FIPPA, it is subject to FIPPA as part of the Ministry of Community Safety and Correctional Services. With regard to municipal police services, while the municipal police service board is the institution under MFIPPA, the police service is subject to MFIPPA as well.

4 Where this guidance refers to police service boards, it should be read as including requirements for both police service boards and the solicitor general who oversees the Ontario Provincial Police.

## WHAT IS ALPR TECHNOLOGY?

Generally, an ALPR system works as follows:

1. The camera automatically captures images of all licence plates within its scanning range. With each capture, two images are produced: one of the licence plate itself, and another contextual image to show the make, model, and colour of the associated vehicle. Contextual images may inadvertently capture images of individuals such as vehicle occupants or pedestrians. Depending on how the system is configured, it may also record the date, time, and geolocation associated with the licence plate image.

2. The computer uses software to analyze the images to extract and digitize the plate information for further processing.

3. When a scanned plate appears to match a plate on a hotlist, the system alerts the police service. An officer then attempts to visually confirm whether the potential hit reflects a match by comparing the image of the vehicle plate to the ALPR system's digitized plate information. A hit may trigger the display of additional vehicle registration information to the officer, such as the vehicle make, model, year and colour, which supports confirmation and action.

4. Where the hit involves a suspended driver who is the plate's registered owner, the system identifies their name and other information, such as whether they require glasses or corrective lenses. The officer may use other systems to clearly identify the vehicle and driver, if the vehicle is stopped and approached.

5. Once the accuracy of the match is manually confirmed, an officer may take action as required, such as conducting a roadside stop and issuing a ticket to the driver for driving with an expired plate, or further verifying whether the vehicle's owner with a suspended licence is actually driving the vehicle.

6. Officers are not alerted to non-hits, and there is no requirement to take action in these cases.

ALPR systems may capture and extract inaccurate licence plate information. For example, mud covering a licence plate could cause it to be misread by the system. Additionally, while the system may capture and extract the correct licence plate number, the issuing province may be incorrect. For these reasons, whether using mobile or fixed ALPR, an officer must confirm hits as valid and actionable.

Depending on how the system is set up, hit information may be recorded on the computer in the police vehicle or recorded on a remote police server.

## TYPES OF ALPR TECHNOLOGY

**Mobile ALPR systems** involve outfitting police vehicles with ALPR technology. Cameras can be mounted to the exterior of a police vehicle to capture images of licence plates both in front of and behind the police vehicle. As an alternative to externally mounted cameras, ALPR software can be integrated into existing in-car camera systems (ICCS). With ICCS, cameras are mounted inside the police vehicle. One camera faces outward to capture footage outside the vehicle, and another camera faces inward, capturing footage inside the police vehicle. Mobile ALPR systems can

continuously scan licence plates while the vehicle is operational, for example, when officers are on vehicle patrol.

**Fixed ALPR systems** involve installing stationary cameras at strategic locations. ALPR cameras can be affixed to highway overhangs, streetlights, telephone or traffic poles, etc. Fixed ALPR systems may operate 24-7 and continuously scan all licence plates that come within range of the camera, even vehicles traveling at high speeds. If multiple fixed ALPR cameras are installed along a single thoroughfare, the data collected can reveal the travel information of a vehicle passing to and from certain locations at specific points in time.

## PERSONAL INFORMATION

Police services must comply with the privacy rules set out in MFIPPA and FIPPA when collecting, retaining, using or disclosing personal information. Section 2(1) of MFIPPA and FIPPA defines personal information as "recorded information about an identifiable individual," which includes, but is not limited to, "any identifying number, symbol or other particular assigned to the individual."

The IPC has ruled that a licence plate number of a vehicle owned by an individual is personal information.[5] Licence plates are assigned to the individual and retained by the individual when their vehicle is sold. Given that the plate is associated with an individual, it can reveal information about that person. Therefore, the rules in MFIPPA and FIPPA regarding personal information generally apply to police services collecting or using licence plate numbers. The location, time and date linked to a licence plate would also be considered personal information. Accordingly, a police service's ALPR system and its associated policies, procedures and technical controls must comply with Ontario's public sector privacy legislation.

## PRIVACY IMPLICATIONS OF ALPR SYSTEMS

While ALPR systems can be useful law enforcement tools, they can also pose significant risks to the privacy of individuals. In addition to complying with MFIPPA and FIPPA, police services must ensure that their ALPR programs respect privacy rights recognized under the *Canadian Charter of Rights and Freedoms*. The Supreme Court of Canada has recognized a right to privacy in public spaces, including on public roads.[6] Proper policies, procedures and technical controls can help ensure that personal information is handled in a lawful manner.

While ALPR technology is not new, the number of police-operated ALPR systems monitoring Ontario roadways has grown significantly in recent years and will likely continue to grow. The expansion of ALPR systems across Ontario and their enhanced capacity to collect more information further exacerbate privacy and surveillance risks, as discussed in the following sections.

More ALPR systems mean more licence plates are being scanned daily, together with contextual information, resulting in exponentially more ALPR data for police to collect, manage, and protect. System or human errors, leading to misreads or misidentifications, may also become more frequent and have unintended and serious implications for individuals. For example, a vehicle registered to a

5 IPC orders **M-336** and **MO-1863**, and IPC privacy investigation **MC-030023-1**.

6 *R v Spencer*, 2014 SCC 43 at para 44; and *R v Wise*, [1992] 1 SCR 527 at 564-565.

suspended driver will trigger a hit on a hotlist. However, the vehicle's registered owner may not be the one driving. Regardless, the officer would receive an alert from the ALPR system, which could result in a roadside stop. This may lead to individuals being repeatedly stopped, potentially impacting secondary drivers or families where vehicles are shared between or within households.

The widespread deployment of ALPR systems across the province has resulted in a more expansive surveillance network, with more granular capacity to track a vehicle and driver's movements by compiling ALPR hits across multiple cameras. As a result, the travel pattern of a driver and their vehicle may be more easily observed by police, especially given these systems record the date, time, and proximate location of vehicles as they are scanned. If this data is retained by police, over time, it may reveal patterns of movement within cities or around the province, allowing inferences to be made about individuals, for example, frequently visited areas or unusual destinations of certain drivers.

Individuals may alter or censor their activities when they are aware of being watched and feel inhibited from participating in lawful activities such as accessing medical services, protesting peacefully or advocating for societal change. ALPR systems have the potential to cause unintended consequences, such as a chilling effect on freedom of speech and association.

As such, police should be transparent and consultative about their use of ALPR, implement detailed policies and procedures, and carefully design and configure their systems to protect the privacy and other fundamental rights of the public.

## SYSTEM CONFIGURATION

Most ALPR systems can be configured in a variety of ways. A police service should configure its ALPR system to mitigate privacy risks and be consistent with the policies and procedures it develops. This includes ensuring the system's cameras capture images of licence plates only and not the vehicle's occupants or pedestrians. Adopting a **privacy by design** approach to proactively embed privacy into the design and configuration of the system from the start is recommended.

Should the system's cameras inadvertently capture more than just the licence plate, any additional personal information should be redacted in accordance with the police service's applicable policies and procedures. This may require blurring of the images to conceal the identity of individuals. To ensure that the amount of personal information collected is limited to what is necessary, the number of cameras and their installation may also need to be adjusted accordingly.

The system should also be configured to prevent tampering or bypassing controls. Users operating an ALPR system should not be able to change or reconfigure the device or system settings without appropriate authorization. The system should log any changes to its configuration.

Police may work with technology vendors to acquire, configure, and implement their ALPR systems, but ultimately remain accountable for complying with Ontario's privacy laws. Police services should refer to the IPC's guidance, ***Privacy and Access in Public Sector Contracting with Third Party Service Providers***, for recommendations related to engaging with third party service providers on privacy and transparency matters.

## CONDUCT A PRIVACY IMPACT ASSESSMENT (PIA)

Before implementing or significantly changing an ALPR program, including pilot programs, police services should assess potential impacts on privacy by conducting a privacy impact assessment (PIA). A PIA assesses the actual and potential impacts of a given program or activity on an individual's privacy and identifies the safeguards and strategies needed to eliminate or reduce these impacts to acceptable levels. Police services should update their PIA before making any material changes to their ALPR program.

The PIA should identify and address issues relating to the use of ALPR technologies, including, but not limited to:

- authority for the use of the system
- purpose and scope of the program, including the criteria governing any hotlists
- authority and scope of the collection, retention, use, disclosure and disposal of personal information
- consideration as to whether an ALPR program is necessary and effective for a police service by clearly identifying the program's objectives and intended uses
- assessment of whether similar outcomes could be achieved through less privacy-invasive methods
- rationale for the number and location of cameras in a given program, especially regarding the placement and installation of any fixed cameras in specific locations
- requirements for public notice and individual access to information
- design and technical controls needed to assure integrity of the system and its operation
- policy controls to assure accountability and oversight
- security measures to safeguard personal information
- periodic reviews and audits of the stated objectives, uses, and the overall effectiveness of the program

Police services may wish to refer to the IPC's ***Planning for Success: Privacy Impact Assessment Guide***, for guidance on completing a PIA.

### ADDITIONAL CONSIDERATIONS FOR FIXED ALPR

Depending on the system's configuration, fixed ALPR systems may continuously capture the licence plate of every vehicle passing a particular location or entering and leaving a specific area. As such, fixed ALPR systems introduce additional privacy and surveillance risks that police services must carefully weigh and consider in their PIA, policies and procedures and during consultation with the public before deployment.

The necessity, proportionality, and transparency surrounding fixed ALPR programs are particularly important to consider. When determining whether fixed ALPR cameras are necessary, police services

should carefully assess the placement and number of proposed fixed cameras to assist officers with immediate roadside enforcement activity. Police services should routinely re-evaluate the locations of cameras to assess for any unintended consequences or negative impacts and re-affirm whether their presence at a particular location is still necessary and proportionate or should be removed.

In particular, police should assess the impact fixed ALPR cameras can have on specific communities if deployed near sensitive sites such as areas associated with protests, places of worship or at the entrances and exits of a town. Combining fixed ALPR systems with existing mobile ALPR systems or other technologies may further increase the complexity and overall privacy risks of a police service's ALPR program.

Public consultations and full disclosure of the intended locations of fixed ALPR camera locations should be carried out before cameras are installed. Recommendations for notice, transparency and public engagement can be found in the policies and procedures section of this document.

## CONSULT THE IPC

To help ensure that privacy issues are appropriately considered and addressed, we encourage police services to consult with the IPC when:

- significantly changing or expanding their ALPR program,[7] especially if considering novel configurations, fixed ALPR systems or combining ALPR with other technologies such as CCTV cameras or video analytics
- considering expanding a hotlist beyond the categories listed in Appendix A and Appendix B
- considering using ALPR data or information for law enforcement purposes outside of assisting officers with immediate roadside enforcement activity

## CONDUCT A PILOT

For police services considering deploying mobile or fixed ALPR systems, or significantly changing their existing ALPR program, a time-limited pilot (also called a test phase) should be conducted before full implementation. A pilot tests for functionality, privacy, security, transparency, and necessity. An evaluation of the pilot results will assist police in making any necessary adjustments to key components of their program, including the PIA, program policies, and procedures.

When planning to conduct a pilot, a police service should:

- define the purpose, goals, objectives, and scope of the pilot
- establish what will be measured during the pilot (for example, appropriate metrics related to system configuration, device functionality, effectiveness of privacy and security controls) and share the results with the public

7 In 2003, the IPC investigated the Toronto Police Service's use of ALPR to find stolen vehicles (see IPC privacy investigation **MC-030023-1**). The IPC stated that institutions, including law enforcement agencies, should consult with the IPC before launching any similar initiatives that may impact privacy.

- establish the appropriate administrative supports for data collection and analysis that will guide the pilot and its evaluation
- consult and inform the public about the pilot and planned next steps, particularly those likely to be impacted by the ALPR program, and seek input from affected organizations, including civil society groups
- articulate a clear rationale for the number and location of cameras required, especially regarding the placement and installation of any fixed cameras in specific locations/communities
- assess and document any operational differences related to responding to hits from mobile versus fixed ALPR systems
- assess whether the intended benefits of the ALPR system were realized and whether any unforeseen risks or harms resulted

## POLICIES AND PROCEDURES

Developing and implementing comprehensive policies and procedures for the use of ALPR systems is crucial. Among other things, ALPR policies and procedures should provide guidance on the appropriate use of the system by officers and other users, including regular reviews and audits. The following section outlines the matters that ALPR policies and procedures should address.

### AUTHORITY, SCOPE AND PURPOSE OF THE PROGRAM

Police services must ensure that they have the legal authority under MFIPPA or FIPPA to collect, retain, use and disclose the personal information involved in the ALPR program. In designing and implementing the program, they should ensure that it will operate in a manner that is consistent with the scope of its roadside-related law enforcement duties and powers. The policies and procedures should identify the specific purposes that justify the use of an ALPR system, including the purposes for which personal information will be used.

### COLLECTION

ALPR systems scan every licence plate that comes into view of the camera. This means an ALPR-equipped vehicle or fixed ALPR camera can collect information about the everyday activities of thousands of individuals. Many of the plates collected will not result in hits and, therefore, will not be relevant to the purpose of the program.

Section 28(2) of MFIPPA and 38(2) of FIPPA prohibit an institution from collecting personal information unless the collection is:

1. expressly authorized by statute
2. used for the purposes of law enforcement
3. necessary to the proper administration of a lawfully authorized activity

An institution must meet at least one of these three conditions to be permitted to collect personal information. In most circumstances, a police service will look to the second condition — **used for the purposes of law enforcement** — when making decisions about the scope, purpose, design and operation of an ALPR program.

To meet the definition of law enforcement in section 2(1) of MFIPPA and FIPPA, the collection must either be used for the purpose of policing or "investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings."

The IPC has ruled that the phrase "used for the purposes of law enforcement" is not an unconditional authority, and only applies in cases where the collection of personal information **furthers actual law enforcement purposes**.[8] With respect to ALPR, personal information collected by police may be used to alert an officer on patrol of the presence of a licence plate in circumstances that would generally justify a roadside stop of a vehicle. This would include situations where the officer confirms that the plate and/or the vehicle is stolen, or that the registered owner of a licence plate has a suspended driver's licence, is uninsured, is wanted under a warrant, or is associated with an Amber Alert.

To administer an ALPR program, police may collect personal information from a third party, such as the MTO, CPIC, or another police service. Personal information collected from the MTO and CPIC includes a daily hotlist of licence plates. Police services may also share licence plates of interest with other police services for matching purposes.

To help ensure compliance with MFIPPA and FIPPA, police services should consider entering into an information-sharing agreement with any third parties. The agreement should clarify legal authorities for sharing information, as well as the rights and obligations of all parties with respect to the handling of personal information. If such an agreement is not already in place, police services should consult with their legal counsel and privacy staff for further guidance.

## NOTICE

MFIPPA and FIPPA require institutions to notify individuals of the collection of their personal information, subject to specific exceptions.[9] In particular, section 29(2) of MFIPPA and 39(2) of FIPPA indicate that the institution must inform the individual of:

a. the legal authority for the collection;

b. the principal purpose or purposes for which the personal information is intended to be used; and

c. the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

Police services should develop and post appropriate notices that are sufficiently transparent to inform the public of their use of ALPR, prior to implementation.

**Visual notice**: For mobile ALPR systems, where practicable, police vehicles equipped with ALPR should be marked with a notice, alerting the public that ALPR is in use.

8 IPC, Privacy Complaint Report **MC-040012-1**.

9 Section 29(3) of MFIPPA and section 39(3) of FIPPA provide exceptions to notice for certain law enforcement purposes. Note that these exceptions apply on a case-by-case basis.

For fixed ALPR systems, signs should be prominently displayed at the perimeter of the monitored area(s). Signs should clearly indicate that a fixed ALPR system is in use and include the information required by paragraphs (a)-(c) of section 29(2) of MFIPPA and section 39(2) of FIPPA, as previously described.

**Verbal notice**: Absent compelling concerns about public safety or officer safety, officers should notify an individual of the use of ALPR when the individual's vehicle is stopped because of a system hit.

## TRANSPARENCY

Police should raise public awareness of the use of ALPR systems through the local media, social media campaigns, and their websites. Further, police services should ensure that the information required by paragraphs (a) to (c) of section 29(2) of MFIPPA and section 39(2) of FIPPA is available and easily accessible on their website.

For fixed ALPR systems, police should consult the public and provide written notice before these systems are installed and operational.

In addition, police services should ensure that up-to-date information about any ALPR program or pilot program is posted on their website, including:

- the most current version of the board's ALPR policies and the service's ALPR procedures
- a description of what information is being collected by ALPR and for what purposes
- a description of the service's ALPR program, including the numbers and types of vehicles equipped with mobile cameras, and locations of fixed cameras
- the applicable retention periods
- how individuals can complain about the use or placement of ALPR cameras or hotlist entries (see section on **Complaint and redress mechanisms**)
- how individuals can make requests to view, access or seek the public release of ALPR scans and associated data
- information about how to appeal to the IPC where an access to information request is denied in whole or in part
- information about how individuals can request access to and correction of their personal information (such as to correct hotlist entries based on erroneous or out-of-date information), and
- a copy of the police service's most recent annual report to its board

## USE

Section 31 of MFIPPA and section 41(1) of FIPPA set restrictions on how personal information may be used once it has been lawfully collected. The acts prohibit the use of personal information unless the institution:

- obtains consent from the individual to whom the information relates;
- uses the personal information for the purpose for which it was obtained or compiled or for a consistent purpose; or
- uses the information for a purpose for which the information may be disclosed to the institution under section 32 of MFIPPA or section 42(1) of FIPPA.

A consistent purpose is defined in section 33 of MFIPPA and section 43 of FIPPA as a use of personal information that the individual to whom the information relates might reasonably have expected at the time of collection. Use of the personal information for other purposes is not permitted, subject to the above-mentioned statutory exceptions.

The personal information held by a police service's ALPR system will generally fall into three categories: hotlists, hit information and, for a very brief time, non-hit information. Police should define how hotlists and hit information may be used, and by whom, to ensure they are only used for authorized purposes. The system should delete non-hit information immediately after it is collected, as described in the following section. Describing how each of these categories of information is managed will help ensure transparency and accountability for their use in an appropriate and privacy-protective manner.

## THE SCOPE OF THE HOTLISTS

Inclusion of a licence plate number on a hotlist may have significant impacts on an individual's privacy rights, and on their right to move freely through the community. Accordingly, ALPR policies and procedures should set strict limits on the scope and design of its hotlists and ensure appropriate oversight.

The content of a hotlist and the permitted categories of plates must be carefully controlled by well-defined, objective standards that are connected to the lawful purpose of the hotlist. Permitted categories of plates collected from the MTO and CPIC are listed in Appendix A. Permitted categories of manual plate entries are listed in Appendix B.[10] Police services should restrict their use of hotlist categories to those listed in Appendix A and Appendix B.

Expanding a hotlist beyond the categories listed in Appendix A and Appendix B may have an unreasonable impact on privacy rights of the individual. If a police service believes it is necessary to include plates outside the scope of any of these categories, they should consult with the IPC prior to doing so.

A police service's ALPR policies and procedures should set out the hotlists in use, the categories of plates permitted on each hotlist and the agency responsible for compiling each hotlist.

## MANUAL ENTRIES

In addition to receiving hotlists from institutions such as the MTO, officers can manually add licence plates to a hotlist. It is important that policies and procedures define the specific and limited circumstances in which licence plates may be manually added or distributed to other police services.

10 Appendix A and B were developed based on the IPC's consultations with the OPP.

For example, a manual entry might be permitted for a plate associated with an Amber Alert or with an individual reported missing. The circumstances where manual changes to a hotlist are allowed should be detailed and complete, with no other types of manual entries permitted. As indicated above, police should restrict their use of manual entries to those categories listed in Appendix B.

ALPR policies and procedures should also set out the specific information that an officer must include when manually entering a licence plate. This includes the officer 's name and unique identification number (such as a badge number), the reason for entering the plate, as well as how long the plate is to remain on the hotlist. An appropriate time frame should be specified in the policy.

The entries should remain on a hotlist only for as long as is reasonably necessary, after which the entry should be removed from all ALPR systems. The policy should also set out whether an entry must be accompanied by physical descriptors of the driver registered to or associated with the plate in the comments field.

Additionally, the policy should consider whether a manual entry should be distributed to the hotlists of all other Ontario ALPR users or be restricted to the individual police service's internal hotlist. However, a manual entry of a plate reasonably believed to be in use by a suspended driver but not registered to them must be restricted to the individual police service's internal hotlist, and not distributed to all other Ontario ALPR users, (see Appendix B).

## MANUAL SEARCHES

While ALPR systems automatically scan for licence plates, the system may permit an officer to manually check if a licence plate is on a hotlist or included in the hits and non-hits captured by the system. As with other police databases such as CPIC, it may be appropriate for a police officer to manually perform such a check. ALPR policies should define the circumstances in which officers are permitted and not permitted to manually search for a plate. For example, policies should prohibit officers from using the manual search function for reasons unrelated to an active and open criminal investigation.

Police should configure ALPR systems to log all manual searches, and the log should include the identity of the officer conducting the search, the date, time, nature of and reason for the manual search and any associated file numbers.

## MANAGING HIT AND NON-HIT INFORMATION

ALPR systems are used to determine whether a plate matches what is on a hotlist. Once an officer visually confirms that a hit is accurate, the hit information may be retained and used for related law enforcement purposes and legal proceedings. For example, if a hit matches a stolen licence plate, the hit information may be used to investigate and prosecute the theft.

Non-hit information should only be collected or used briefly and only as necessary to determine if a scanned licence plate is a hit versus a non-hit. Once a scan is determined to be a non-hit, its collection, retention or use is no longer permitted under MFIPPA or FIPPA.

Non-hit data should be immediately deleted as soon as technologically feasible and should not be accessed or used before it is deleted unless such access or use is clearly authorized by law. Before accessing or using any non-hit data, police should consult with their legal counsel to help determine whether they have the necessary legal authority to do so (e.g., under a production order). In the meantime, while police may preserve a limited subset of non-hit data long enough to determine the legal authority issue (e.g., non-hit data associated with a specific location or defined area, a specific timeframe, and a specific and related criminal investigation), all other non-hit data should be immediately deleted. As soon as the legal authority issues have been resolved, any preserved non-hit data that police are not authorized to access or use should also be deleted immediately.

## SECONDARY USES OF ALPR HIT INFORMATION

Police should only use hit information collected as part of the ALPR program for the program's specific and defined law enforcement purposes. Specifically, for alerting an officer on patrol to the presence of a licence plate matching one on a hotlist in circumstances that would justify a roadside stop of a vehicle and enabling subsequent related investigation and enforcement activities.

Police should not use any ALPR information, including hit information, for any secondary purpose, such as the real-time tracking or historical mapping of the location and movements of an individual unless such a secondary purpose is clearly authorized by law.

## INTERNAL ACCESS TO THE ALPR SYSTEM

Within a police service, access to an ALPR system should be restricted to a limited number of pre-authorized individuals. These individuals should be subject to role-based access controls that are documented and issued on a need-to-know basis. It is also important that each instance of access to and use of the ALPR system be logged. Log files should identify the individual user accessing the system by name and unique identification number (such as badge number) and record the time of access, the information accessed, and the specific reason for accessing and using the system.

## DISCLOSURE

MFIPPA and FIPPA prohibit the disclosure of personal information except in the circumstances identified in section 32 of MFIPPA and 42(1) of FIPPA. As with the use of personal information, the acts permit a police service to disclose personal information for the purposes for which it was obtained or compiled or for a consistent purpose. ALPR policies and procedures should set out when personal information collected by the system may be disclosed.

Police services should also maintain a log of each disclosure, which should include the following information:

- the legal authority for the disclosure, including a description of the circumstances justifying the disclosure, including references to applicable information sharing agreement(s)
- the identity of the officer who has authorized the disclosure

- the date, time and location of the original collection
- any linked or appended records associated with the plate
- the name and title of the third party to whom the information is disclosed, and, where applicable, the case file number of the disclosing party and/or the third party's investigation
- a description of the information involved, such as the numbers of plates being disclosed and from which types or categories of hotlist
- the means used to disclose the information
- a description of any conditions that restrict the third party's right to use and disclose the information
- whether the information will be securely returned or securely destroyed by the recipient after use

## RETENTION

MFIPPA, FIPPA and their regulations set out rules regarding the minimum length of time institutions must retain personal information once they have used it. Specifically, section 5 of Regulation 823 of MFIPPA and section 5(1) of Regulation 460 of FIPPA require institutions to retain this information for at least one year after use unless the individual consents to earlier destruction. Regulation 823 of MFIPPA permits municipal institutions to reduce this time period through a resolution or by-law. Once ALPR information is determined to be a hit and the hit has been confirmed, the police service must retain it in compliance with these rules. Of course, as hit information may be relevant to a specific investigation or proceeding, there may be other retention requirements beyond those set out in these regulations.

In contrast to hit information, police should immediately delete any non-hit information as soon as technologically feasible, whether it resides in the vehicle's computer or a police server. (See section on **Managing hit and non-hit information**).

Police services should amend their information practices, bylaws, resolutions, etc., to ensure compliance with these requirements.

## ACCURACY

Police services should update all hotlist databases stored on central servers and police vehicle computers as often as necessary to ensure that they are accurate and up to date.[11] Most ALPR systems can be configured to support daily updates. Once an entry is removed from any hotlist, it should be deleted from all other ALPR hotlists as soon as possible. In addition, ALPR policies, procedures and systems should be configured to facilitate the routine purging of duplicate, expired and erroneous hotlist entries. Updates to databases should be logged for accountability purposes.

## SECURITY

Section 3 of Regulation 823 of MFIPPA and section 4 of Regulation 460 of FIPPA require institutions to define, document and put in place reasonable measures to prevent unauthorized access as well

11 Note that section 30(3) of MFIPPA and section 40(3) of FIPPA provide exceptions for law enforcement to the act's accuracy requirements.

as inadvertent destruction or damage to records. Therefore, police services must implement policies and procedures to ensure the secure handling of personal information.

Police services should implement the following security measures:

- ***Secure transfer***: Ensure information is secure during transfers to servers, and between servers and police vehicles
- ***Secure storage***: Encrypt ALPR information when not in use, regardless of storage location
- ***Physical security***: Store physical ALPR equipment and records, such as discs, memory cards or servers, securely to prevent theft, loss or unauthorized access. Consider the security and placement of ALPR cameras at fixed locations, to prevent tampering, damage, loss, theft, or unauthorized access
- ***Access controls***: Limit all access to ALPR information to individuals that require the information for their role
- ***Secure deletion***: Ensure that outdated, inaccurate or excessive information is permanently destroyed
- ***Data minimization***: Design, configure and operate the ALPR system in a way that restricts personal information from being collected, retained, used and disclosed any more than necessary
- ***Configuration***: Standardize secure system configurations across the service's ALPR systems, and do not use default or factory settings
- ***Maintenance***: Patch systems and applications regularly to protect against vulnerabilities
- ***Logging***: Keep audit logs of all accesses, uses and disclosures of ALPR information. Such logs should be generated automatically when records are maintained electronically
- ***Operations monitoring***: Monitor ALPR system performance and respond to all suspected privacy and security breaches, incidents and system behaviour that is out of the ordinary
- ***Risk assessment***: Carry out regular risk assessments and other operational reviews to assess and improve the effectiveness of security measures

Police services should implement protocols to identify, contain, investigate and remediate security and privacy breaches that may arise. The IPC's ***Privacy Breaches: Guidelines for Public Sector Organizations*** provides guidance on developing breach management procedures.

## REVIEWS AND AUDITS

Operational monitoring is essential to an accountable and privacy-protective ALPR program. Regular reviews and audits should be conducted to evaluate and improve an ALPR program.

Police services should routinely monitor system access logs for unusual behaviour and breaches of the policies and procedures. This should include random reviews of individual users. Officers should be informed that their activities are subject to audit or monitoring and that they may be called upon to justify their use of the system.

Police services should regularly review the technology, system controls and operational performance of ALPR programs to ensure that they:

- continue to be effective
- comply with policies and procedures, and
- remain necessary and proportionate.

Further, ALPR policies and procedures should be reviewed regularly and updated whenever there is a significant change to the ALPR system. An independent third party could conduct these reviews, and any identified deficiencies or concerns should be addressed as soon as possible.

Police services should also consider publishing an annual report on their use of ALPR systems, describing the program's objectives, deployment activities, key operational metrics and statistics. Reports provide transparency on the use of these systems and demonstrating their success may increase public support for the program.

## TRAINING

Effective operation of the ALPR system and compliance with MFIPPA and FIPPA depends on adherence to policies and procedures. Therefore, police services must ensure appropriate training for everyone who has access to the system.

Initial and ongoing training should include clear instructions on roles, duties, obligations and other responsibilities. Users (officers, other employees and/or third party service providers) should be provided with policies and procedures and should sign an agreement to adhere to the defined practices, including an undertaking of confidentiality. Training should include a discussion of disciplinary measures that could be taken should any party violate the police service's policies and procedures.

All applicable policies and procedures should be communicated and made available to officers, IT administrators and other staff involved in the operation of the program, as well as any third party service providers.

## COMPLAINT AND REDRESS MECHANISMS

ALPR policies and procedures should provide information about how individuals can make a complaint and request removal from the system when they believe their licence plate should not be on a hotlist. Where the individual's hotlist entry was compiled by another police service, another institution or another agency, such as the Royal Canadian Mounted Police, members of the public should be provided with the name and contact information of the official responsible for hotlist entries and responses to complaints and/or requests for redress, or removal.

Police should also inform the public of their right to make a privacy complaint to the IPC in accordance with MFIPPA and FIPPA, as applicable.

Police services should make the above information readily available to members of the public on their website, together with all other relevant information about their ALPR policies and procedures.

## ACCESS TO INFORMATION REQUESTS

In Ontario, individuals have a right of access to records in the custody or control of institutions under section 4 of MFIPPA and section 10 of FIPPA. Additionally, individuals whose personal information is in the custody or control of institutions have a right to access and correct their personal information under section 36(1) of MFIPPA and section 47(1) of FIPPA.

A police service may receive a request from an individual seeking confirmation of whether, for example, their licence plate is, or was, on a hotlist, or for access to records associated with the collection, use or disclosure of their licence plate. Accordingly, a police service must have a process in place to facilitate responses to access requests within the legislated timeframe.

Note that while individuals have a right to request access to such records, all or portions of the records requested may be exempt from disclosure under MFIPPA and FIPPA. For example, section 38 of MFIPPA and section 49 of FIPPA set out these exemptions, including where the disclosure would constitute an unjustified invasion of another individual's privacy. Police services should look to their freedom of information and protection of privacy coordinator for guidance regarding the appropriate response to a request for access.

In cases where the police service denies an access to information request, it should inform the requester of their right to file an appeal with the IPC.

# CONCLUSION

ALPR systems assist police in the timely identification of licence plates on hotlists for the purpose of conducting further investigation and enforcement. Police use of ALPR continues to expand which raises significant privacy and surveillance implications. ALPR systems can collect, retain, and use personal information about individuals as they go about their everyday lives. Fixed ALPR systems, in particular, may continuously be recording every licence plate that passes a specific location or within a certain range. The resulting intrusion on privacy can have significant implications for fundamental rights and liberties. Therefore, proper policies, procedures and technical controls must be in place to ensure the privacy, security, functionality and necessity of the ALPR program, whether mobile or fixed.

If an ALPR program is implemented in a lawful, transparent and privacy-protective manner, as described in these guidelines, the risks to privacy and other rights may be sufficiently mitigated for police services to meet their public safety objectives, while also being able to meet their obligations under MFIPPA and FIPPA.

## APPENDIX A: CATEGORIES OF PLATES GATHERED FROM THE MINISTRY OF TRANSPORTATION (MTO) AND THE CANADIAN POLICE INFORMATION CENTRE (CPIC)

Information provided by MTO:

- Plates with expired licence plate stickers
- Terminated plates
- Plates reported missing, lost or stolen
- Suspended plates in registrants' possession or MTO's possession
- Un-issued plates and un-issued stolen plates
- Spoiled stock
- Unattached plates
- Plates registered to suspended drivers
- Plates registered to unlicensed drivers

Information provided by CPIC:

- Stolen plates
- Plates associated with stolen vehicles (stolen autos, trucks and motorcycles)
- Plates registered to persons wanted under a warrant

# APPENDIX B: CATEGORIES OF MANUAL PLATE ENTRIES

- A plate registered to a person who is under investigation in an open and active criminal case
- A plate directly connected to criminal activity in an open and active criminal investigation
- A plate registered to a person who has been served a short-term driver's licence suspension for an alcohol or *Highway Traffic Act* related infraction and it is believed that the person may continue to operate a vehicle during the suspension period
- A plate associated with a person who has been reported missing
- A plate associated with an Amber Alert
- A plate not registered to but reasonably believed to be in use by a suspended driver whose driving record under the *Highway Traffic Act* raises public safety concerns. The manual entry must:
    - be restricted to the individual service's internal hotlist only, and **not** distributed to all other ALPR users
    - remain on the service's internal hotlist for no more than thirty days, after which the entry is to be removed, and
    - be accompanied by physical descriptors of the suspended driver in the "comments" field to assist in distinguishing the suspended driver from other individual drivers including the registered owner of the plate

## APPENDIX C: SUMMARY OF KEY RECOMMENDATIONS

*Below is a summary of key recommendations, for reference purposes only. Please consult the corresponding section of this guidance document for further details and specific requirements.*

When implementing an automated licence plate recognition (ALPR) program in Ontario, the IPC recommends the following for police services.

### SYSTEM CONFIGURATION

- Configure the ALPR system to mitigate privacy risks and be consistent with the policies and procedures the police service develops. This includes ensuring the system's cameras capture images of licence plates only and not occupants of the vehicle or pedestrians.
- Adopt a privacy by design approach to proactively embed privacy into the design and configuration of the system from the start.
- Should the system's cameras inadvertently capture more than just the licence plate, any personal information should be redacted in accordance with applicable policies and procedures.
- To ensure that the amount of personal information collected is limited to that which is necessary, the number of cameras and their installation may also need to be adjusted accordingly.
- The system should also be configured to prevent tampering or bypassing controls.
- Users operating an ALPR system should not be able to change or reconfigure the device or system settings without appropriate authorization.
- The system should log any changes to its configuration.

### CONDUCT A PRIVACY IMPACT ASSESSMENT (PIA)

- Before implementing or significantly changing an ALPR program, including pilot programs, police services should assess potential impacts on privacy by conducting a PIA.
- Police services should update their PIA before any material changes are made to their ALPR program.
- The PIA should identify and address privacy issues relating to the use of ALPR technologies, including additional considerations for fixed ALPR systems, as discussed in this guidance.

### CONSULT THE IPC

- To help ensure that privacy issues are appropriately considered and addressed, police services are encouraged to consult with the IPC when:
    - significantly changing or expanding their ALPR program, especially if considering novel configurations, fixed ALPR systems or combining ALPR with other technologies such as CCTV cameras or video analytics;

- considering expanding a hotlist beyond the categories listed in Appendix A and Appendix B; or
- considering using ALPR data or information for law enforcement purposes outside of assisting officers with immediate roadside enforcement activity.

## CONDUCT A PILOT

- For police services considering deploying mobile or fixed ALPR systems, or significantly changing their existing ALPR program, a time-limited pilot (also called a test phase) should be conducted before full implementation.
- An evaluation of the results of the pilot will assist in making any necessary adjustments to key components of their program, including the PIA, program policies, and procedures.
- When planning to conduct a pilot, police services should address the matters outlined in this guidance.

## POLICIES AND PROCEDURES

- Developing and implementing comprehensive policies and procedures for the use of ALPR systems is crucial.
- ALPR policies and procedures should provide guidance on the appropriate use of the system by officers and other users, including regular reviews and audits.

## AUTHORITY, SCOPE, AND PURPOSE OF THE PROGRAM

- Police services must ensure that they have the legal authority under MFIPPA or FIPPA to collect, retain, use and disclose the personal information involved in the ALPR program.
- In designing and implementing the program, they should ensure that it will operate in a manner that is consistent with the scope of its roadside-related law enforcement duties and powers.
- The policies and procedures should identify the specific purposes that justify the use of an ALPR system, including the purposes for which personal information will be used.

## COLLECTION

- An institution must meet at least one of the three conditions in Section 28(2) of MFIPPA and 38(2) of FIPPA to be permitted to collect personal information.
- To help ensure compliance with MFIPPA and FIPPA, police services should consider entering into an information-sharing agreement with any third parties.
- The agreement should clarify legal authorities for sharing information, as well as the rights and obligations of all parties with respect to the handling of personal information.

- If such an agreement is not already in place, police services should consult with their legal counsel and privacy staff for further guidance.

## NOTICE

- Institutions are required to notify individuals of the collection of their personal information, subject to specific exceptions.
- Police services should develop and post appropriate notices that are sufficiently transparent to inform the public of their use of ALPR, prior to implementation. This includes both visual and verbal notice.
- **Visual notice**:
    - For mobile ALPR systems, where practicable, police vehicles equipped with ALPR should be marked with a notice, alerting the public that ALPR is in use.
    - For fixed ALPR systems, signs should be prominently displayed at the perimeter of the monitored area(s). Signs should clearly indicate that a fixed ALPR system is in use and include the information required by paragraphs (a) to (c) of section 29(2) of MFIPPA and section 39(2) of FIPPA, outlined within this guidance.
- **Verbal notice**:
    - Absent compelling concerns about public safety or officer safety, officers should notify an individual of the use of ALPR when the individual's vehicle is stopped because of a system hit.

## TRANSPARENCY

- Police services should raise public awareness of the use of ALPR systems through the local media, social media campaigns and their websites.
- Police services should ensure that the information required by paragraphs (a) to (c) of section 29(2) of MFIPPA and section 39(2) of FIPPA is available and easily accessible on their website.
- For fixed ALPR systems, police services should consult the public and provide written notice before these systems are installed and operational.
- Police services should ensure that up-to-date information about any ALPR program or pilot program is posted on their website, including the items outlined in this guidance.

## USE

- The personal information held by a police service's ALPR system will generally fall into three categories: hotlists, hit information and, for a very brief time, non-hit information. Police services should define how hotlists and hit information may be used and by whom to ensure they are only used for authorized purposes.

- The system should delete non-hit information immediately after it is collected.
- Describing how each of these categories of information is managed will help ensure transparency and accountability for their use in an appropriate and privacy-protective manner.

## THE SCOPE OF THE HOTLISTS

- A police service's ALPR policies and procedures should set strict limits on the scope and design of its hotlists and ensure appropriate oversight.
- The content of a hotlist and the permitted categories of plates must be carefully controlled by well-defined, objective standards that are connected to the lawful purpose of the hotlist.
- Police services should restrict their use of hotlist categories to those listed in Appendix A and Appendix B.
- If a police service believes it is necessary to include plates outside the scope of any of these categories, they should consult with the IPC prior to doing so.
- A police service's ALPR policies and procedures should set out the hotlists in use, the categories of plates permitted on each hotlist and the agency responsible for compiling each hotlist.

## MANUAL ENTRIES

- It is important that policies and procedures define the specific and limited circumstances in which licence plates may be manually added or distributed to other police services.
- The circumstances where manual changes to a hotlist are allowed should be detailed and complete, with no other types of manual entries permitted.
- Police services should restrict their use of manual entries to those categories listed in Appendix B.
- ALPR policies and procedures should also set out the specific information that an officer must include when manually entering a licence plate.
- The entries should remain on a hotlist only for as long as is reasonably necessary, after which the entry should be removed from all ALPR systems.
- Policies services should consider whether a manual entry should be distributed to the hotlists of all other Ontario ALPR users or be restricted to the individual police service's internal hotlist.
- A manual entry of a plate reasonably believed to be in use by a suspended driver but not registered to them **must** be restricted to the individual police service's internal hotlist, and not distributed to all other Ontario ALPR users, (see Appendix B).

## MANUAL SEARCHES

- ALPR policies should define the circumstances in which officers are permitted and not permitted to manually search for a plate.
- Policies should prohibit officers from using the manual search function for reasons unrelated to an active and open criminal investigation.
- Police services should configure ALPR systems to log all manual searches, and the log should include the identity of the officer conducting the search, the date, time, nature of and reason for the manual search and any associated file numbers.

## MANAGING HIT AND NON-HIT INFORMATION

- Once an officer visually confirms that a hit is accurate, the hit information may be retained and used for related law enforcement purposes and legal proceedings.
- Non-hit information should only be collected or used briefly and only as necessary to determine if a scanned licence plate is a hit versus a non-hit.
- Non-hit data should be immediately deleted as soon as technologically feasible and should not be accessed or used before it is deleted unless such access or use is clearly authorized by law.
- Before accessing or using any non-hit data, police services should consult with their legal counsel to help determine whether they have the necessary legal authority to do so.
- In the meantime, while police services may preserve a limited subset of non-hit data long enough to determine the legal authority issue, all other non-hit data should be immediately deleted.
- As soon as the legal authority issues have been resolved, any preserved non-hit data that police services are not authorized to access or use should also be deleted immediately.

## SECONDARY USES OF ALPR INFORMATION

- Police services should only use hit information collected as part of the ALPR program for the program's specific and defined law enforcement purposes. Specifically, for alerting an officer on patrol to a licence plate matching one on a hotlist in circumstances that would justify a roadside stop of a vehicle and enabling subsequent related investigation and enforcement activities.
- Police services should not use any ALPR information, including hit information, for any secondary purpose, such as the real-time tracking or historical mapping of the location and movements of an individual unless such a secondary purpose is clearly authorized by law.

## INTERNAL ACCESS TO THE ALPR SYSTEM

- Within a police service, access to an ALPR system should be restricted to a limited number of pre-authorized individuals who are subject to role-based access controls that are documented and issued on a need-to-know basis.

- Each instance of access to and use of the ALPR system should be logged.
- Log files should identify the individual user accessing the system by name and unique identification number (such as badge number) and record the time of access, the information accessed, and the specific reason for accessing and using the system.

## DISCLOSURE

- ALPR policies and procedures should set out when personal information collected by the system may be disclosed.
- Police services should also maintain a log of each disclosure, which should include the information outlined in this guidance.

## RETENTION

- Once ALPR information is determined to be tied to a hit and the hit has been confirmed, the police service must retain it in compliance with MFIPPA and FIPPA and its regulations.
- In contrast to hit information, police services should immediately delete any non-hit information as soon as technologically feasible, whether it resides in the vehicle's computer or a police server.
- Police services should amend their information practices, by-laws, resolutions, etc. to ensure compliance with these requirements.

## ACCURACY

- Police services should update all hotlist databases stored on central servers and police vehicle computers as often as necessary to ensure that they are accurate and up to date.
- Once an entry is removed from any hotlist, it should be deleted from all other ALPR hotlists as soon as possible.
- ALPR policies, procedures and systems should be configured to facilitate the routine purging of duplicate, expired and erroneous hotlist entries.
- Updates to databases should be logged for accountability purposes.

## SECURITY

- Police services must implement policies and procedures to ensure the secure handling of personal information.
- Police services should implement the security measures outlined in this guidance, including secure transfer, secure storage, physical security, access controls, secure deletion, data minimization, configuration, maintenance, logging, operations monitoring and risk assessments.

- Police services should implement protocols to identify, contain, investigate and remediate security and privacy breaches that may arise.

## REVIEWS AND AUDITS

- Regular reviews and audits should be conducted to evaluate and improve an ALPR program.
- Police services should routinely monitor system access logs for unusual behaviour and breaches of the policies and procedures. This should include random reviews of individual users.
- Police services should regularly review the technology, system controls and operational performance of ALPR programs to ensure that they:
    - continue to be effective,
    - comply with policies and procedures, and
    - remain necessary and proportionate.
- ALPR policies and procedures should be reviewed regularly and updated whenever there is a significant change to the ALPR system. An independent third party could conduct these reviews, and any identified deficiencies or concerns should be addressed as soon as possible.
- Police services should also consider publishing an annual report on their use of ALPR systems, describing the program's objectives, deployment activities, key operational metrics and statistics.

## TRAINING

- Police services must ensure appropriate training for everyone who has access to the system.
- Initial and ongoing training should include clear instructions on roles, duties, obligations, and other responsibilities.
- Users (officers, other employees, and/or third party service providers) should be provided with policies and procedures and should sign an agreement to adhere to the defined practices, including an undertaking of confidentiality.
- Training should include a discussion of disciplinary measures that could be taken should any party violate the police service's policies and procedures.
- All applicable policies and procedures should be communicated and made available to officers, IT administrators and other staff involved in the operation of the program, as well as any third party service providers.

## COMPLAINT AND REDRESS MECHANISMS

- ALPR policies and procedures should provide information about how individuals can make a complaint and request removal from the system when they believe their licence plate should not be on a hotlist.

- Where the individual's hotlist entry was compiled by another police service, another institution or another agency, such as the RCMP, members of the public should be provided with the name and contact information of the official responsible for hotlist entries and responses to complaints and/or requests for redress, or removal.
- Police services should also inform the public of their right to make a privacy complaint to the IPC in accordance with MFIPPA and FIPPA, as applicable.
- Police services should make the above information readily available to members of the public on their website, together with all other relevant information about their ALPR policies and procedures.

## ACCESS TO INFORMATION REQUESTS

- A police service must have a process in place to facilitate responses to access to information requests within the legislated timeframe.
- Police services should look to their freedom of information and protection of privacy coordinator for guidance regarding the appropriate response to a request for access.
- In cases where the police service denies an access to information request, it should inform the requester of their right to file an appeal with the IPC.

# Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

December 2024