TECHNOLOGY

JULY 2017

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 and providing helpful comments.

CONTENTS

INTRODUCTION

Automated licence plate recognition (ALPR) technologies can quickly capture and match large volumes of licence plate numbers to lists of plates stored in a database. ALPR components that work together, such as a camera, computer and database, form an "ALPR system."[1] Police services in Ontario are using ALPR systems to match licence plates with lists of plates, such as stolen and expired plates, and plates registered to suspended drivers.

ALPR systems can also be set up to capture other information, including the location of vehicles at specific times and dates. As a result, these systems have the potential to be used to track individuals' locations over time, making it easier for police to conduct surveillance and profiling.

The use of ALPR systems raises significant privacy concerns. Among those concerns are potential failures to comply with Ontario's public sector privacy legislation, and intrusions on other fundamental rights and liberties. Proper policies, procedures and technical controls are critical to protecting privacy, particularly when considering that most drivers are law-abiding individuals simply going about their everyday activities.

The Information and Privacy Commissioner of Ontario (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).[2] The IPC has done considerable work relating to ALPR systems. In 2003, we investigated the Toronto Police Service's (TPS) use of ALPR to find stolen vehicles.[3] The IPC was also consulted by the OPP in the development of its ALPR project in 2008, and we continue to work with the OPP with regard to its ALPR system. We have since received a number of inquiries about similar systems from municipal police services.

This document outlines the key obligations of police services under *MFIPPA* and *FIPPA* in their use of ALPR systems and provides guidance, including best practices, on using these systems in a privacy-protective manner. It addresses the use of ALPR systems by police for public safety purposes, in particular for the purpose of alerting an officer in an ALPR-equipped vehicle to the presence of a particular licence plate. It does not cover the use of ALPR systems for traffic management, road tolls or parking enforcement purposes. A different set of privacy issues and mitigation approaches may need to be considered in those contexts. Also, legal obligations and limitations beyond those set out in *MFIPPA* and *FIPPA* may apply to police ALPR systems and should be considered.

DEFINITIONS

- **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.

1 ALPR systems are also known as mobile licence plate recognition systems and automatic number plate recognition systems.

2 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.

3 IPC Privacy Investigation **MC-030023-1**.

- **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 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.
- **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 includes plate images, date, time and geolocation.
- **Police service** refers to a municipal police service, a municipal police services board and the OPP.

WHAT IS ALPR TECHNOLOGY?

ALPR systems include a camera, a computer and a database. Generally, an ALPR system works as follows:

1. A camera mounted on a police vehicle automatically captures images of all licence plates within the camera's scanning range. 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 in the police vehicle 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 officer in the police vehicle. The officer then attempts to confirm whether the hit reflects a match between a licence plate on the list and the vehicle plate by comparing the image of the plate to the ALPR system's digitized plate information. A hit generally triggers the display of additional vehicle registration information to the officer, such as the vehicle make, model, year and colour, which supports confirmation and action. In the case of a hit related to a suspended driver who is the plate's registered owner, the system identifies whether the registered owner is, for example, a male or female and whether they require glasses or corrective lenses. The officer may use other systems to clearly identify the vehicle and driver if and when the vehicle is stopped and approached. Officers are not alerted to non-hits, and there is no requirement to take action in these cases.
4. Once the accuracy of the match is manually confirmed, the officer may take action as required, such as 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.

ALPR systems may also 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, an officer must confirm hits as valid and actionable.

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

PERSONAL INFORMATION

Police services must comply with the privacy rules set out in *MFIPPA* and *FIPPA* when they are 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.[4] Licence plates are assigned to the individual and retained by the individual when his or her vehicle is sold. Given that the plate is associated with the 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.[5] Proper policies, procedures and technical controls can help ensure that personal information is handled in a lawful manner.

Without adequate controls, ALPR systems can enable surveillance and profiling when collecting information such as the date, time and geolocation of vehicles. Such surveillance may reveal other sensitive personal information about individuals, such as their appointment at a doctor's office or participation in a political protest. Individuals may censor their activities when they are aware of being watched and feel inhibited from participating in lawful activities such as protesting peacefully or advocating for societal change. An improperly configured ALPR system has the potential to cause unintended consequences, such as a chilling effect on freedom of speech and association. As such, police should implement detailed policies and procedures, and carefully design and configure their ALPR systems, to protect the privacy and other fundamental rights of the public.

CONDUCT A PRIVACY IMPACT ASSESSMENT (PIA)

Before implementing an ALPR program, police services should assess its potential impact on privacy by conducting a PIA. A PIA identifies the actual and potential effects of a given program or activity on an individual's privacy and the safeguards and strategies needed to eliminate or reduce the negative effects to acceptable levels. Police services should update their PIA before any material changes are made to the system.

4 IPC Orders **M-336** and **MO-1863**, and IPC Privacy Investigation **MC-030023-1**.

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

The PIA should identify issues relating to the use of ALPR technologies, including:

- authority for the use of the system
- purposes 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
- 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
- security measures to safeguard personal information

Police services may wish to refer to the IPC's *Planning for Success: Privacy Impact Assessment Guide*[6] or the Ontario Ministry of Government and Consumer Services' PIA guidelines and tools[7] for completing a PIA.

CONSULT THE IPC

To help ensure that privacy issues are appropriately considered and addressed, we encourage police services to consult with the IPC before implementing or significantly changing an ALPR system.[8] The IPC can help police services to mitigate the privacy impacts that may arise from an ALPR program.

IMPLEMENTATION GUIDELINES

Developing and implementing comprehensive policies and procedures for the use of these systems is crucial. Among other things, ALPR policies and procedures should provide guidance on the appropriate use of the system by officers and include 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.

---

6 IPC's **Planning for Success: Privacy Impact Assessment Guide**.

7 Available by contacting the Information, Privacy and Archives Division by email at **web.foi.MGCS@ontario.ca** or by telephone at 416-212-7061.

8 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.

COLLECTION

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 have the legal authority to collect personal information. In most circumstances, a police service's authority to collect personal information for an ALPR program will lie with the second condition — *used for the purposes of law enforcement*.

Applying 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*.[9] 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 subject to a warrant for his or her arrest or is associated with an Amber Alert.

ALPR systems scan every licence plate that comes into view of the camera. This means an ALPR-equipped vehicle will collect information about the everyday activities of law-abiding individuals. Many of the plates collected will not result in hits and, therefore, will not be relevant to the purpose of the system. Consequently, an important aspect of managing an ALPR system involves limiting the retention of non-hit information.

To administer an ALPR program, police may collect personal information from a third party, such as MTO or CPIC. Personal information collected from these parties includes a daily hotlist of licence plates to be used for matching purposes.

To help ensure compliance with *MFIPPA* and *FIPPA*, police services should consider entering into an information-sharing agreement with any such third parties. The agreement should clarify 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 staff responsible for privacy for further guidance.

9 IPC Privacy Complaint Report **MC-040012-1**.

NOTICE

MFIPPA and *FIPPA* require institutions to notify individuals of the collection of their personal information, subject to specific exceptions.[10] In particular, section 29(2) of *MFIPPA* and 39(2) of *FIPPA* provide 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 notify the public prior to implementing an ALPR system. Police can raise public awareness of the use of ALPR systems through the local media, social media campaigns and their websites. Where practicable, police vehicles equipped with ALPR systems should be marked with a notice, alerting the public that an ALPR system is in use. Further, absent exceptional circumstances, officers should notify an individual of the use of ALPR when the individual's vehicle is stopped as a result of a system hit. Police services should ensure that the information required by paragraphs (a)–(c) of section 29(2) of *MFIPPA* and section 39(2) of FIPPA is available and easily accessible on their website.

Police should also inform the individual of how to challenge their status on a hotlist if they choose to do so. This is discussed in more detail below.

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 non-hit information. The system should delete non-hit information immediately after it is collected, as described below. Police should define how hotlists and hit information may be used and by whom to ensure they are only used for authorized

10 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.

purposes. This will ensure that both of these categories of information are managed in an appropriate and privacy-protective manner.

THE SCOPE OF THE HOTLISTS

Inclusion on a hotlist may have significant impacts on an individual's privacy rights, and on their right to move freely through the community. Accordingly, an ALPR policy 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 MTO and CPIC are listed in Appendix A. Permitted categories of manual plate entries are listed in Appendix B, and are discussed in more detail below. Appendix A and Appendix B were developed on the basis of our consultations with the OPP. 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.

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 plates 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 make the above information, as well as information about their ALPR policies and procedures, readily available to members of the public on their website.

MANUAL ENTRIES

In addition to receiving hotlists from institutions such as MTO, officers may be able to 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. 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, such as the officer's name and 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 an entry should be distributed to the hotlists of all other Ontario ALPR users or restricted to the police vehicle used by the officer who entered the plate. However, note that a manual entry of a plate not registered to but reasonably believed to be in use by a suspended driver *must* be restricted to the current vehicle's hotlist, and not distributed to all other 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 and the date, time, nature of and reason for the manual search.

MANAGING HIT AND NON-HIT INFORMATION

Given that ALPR systems are used to determine whether a plate is on a hotlist, plates that are not on a hotlist, or "non-hits," may not be used for other purposes, or disclosed to another party.

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.

SECONDARY USES OF ALPR INFORMATION

Police should only use information collected as part of the ALPR program for the program's specific and defined law enforcement purposes. These may include alerting an officer on patrol to the presence of a licence plate in circumstances that would justify a roadside stop of a vehicle, and enabling subsequent investigation and enforcement activities. Police should not use ALPR information for secondary purposes, such as tracking the location and movements of law-abiding individuals.

INTERNAL ACCESS TO THE ALPR SYSTEM

Within a police service, access to an ALPR system should be restricted to limited, pre-authorized individuals by implementing appropriate role-based access controls. It is important that all accesses to and uses of the ALPR system be logged and limited to a need-to-know basis. Log files should identify the officer by name and badge number, and record the time of access, the information accessed and the reason for the access to and use of 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
- 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 tied to 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 may only store non-hit information briefly, whether on the vehicle or the server. Non-hit information should be purged as soon as possible.

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 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 also 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
- *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

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.

Police services should implement protocols to identify, contain, investigate and remediate security and privacy breaches that may arise. The IPC's *Privacy Breach Protocol & Guidelines for Government Organizations*[12] 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 are effective and comply with policies and procedures. 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 policies and procedures should be communicated and made available to officers, IT administrators and other staff involved in its operation, as well as any third party service providers.

12 IPC's **Privacy Breach Protocol & Guidelines for Government Organizations**.

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 of access to that 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 or not, 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 several exemptions. These include 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.

SYSTEM CONFIGURATION

Most ALPR systems can be configured in a variety of ways. A police service should configure its ALPR system to be consistent with the policies and procedures it develops to mitigate privacy risks. This includes ensuring the system's cameras capture the licence plate only and not the driver or passengers in the vehicle. The system should also be configured to prevent tampering or bypassing controls. Officers operating an ALPR system should not be able to change or reconfigure device settings without appropriate authorization. The system should log any changes to its configuration.

CONCLUSION

Police services are looking to ALPR systems to assist in the timely identification of licence plates on hotlists for the purpose of conducting further investigation and enforcement. ALPR systems are able to collect, retain and use personal information about law-abiding individuals as they go about their everyday lives. The resulting intrusion on privacy could have significant implications for fundamental rights and liberties. Therefore, proper policies, procedures and technical controls must be in place. If the ALPR program is implemented in a privacy-protective manner, as described in these guidelines, the risks to privacy and other rights may be sufficiently mitigated, and police services will be in a position to meet their obligations under *MFIPPA* and *FIPPA*.

APPENDIX A:

Categories of plates gathered from MTO and 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 an open and active criminal investigation
- 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 distributed to "current user only" (only to the one police vehicle and NOT any other ALPR vehicles)
    - remain in the vehicle's system 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

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

July 2017