Office of the Information & Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

INVESTIGATION REPORT F12-04

USE OF AUTOMATED LICENCE PLATE RECOGNITION TECHNOLOGY BY THE VICTORIA POLICE DEPARTMENT

Elizabeth Denham
Information and Privacy Commissioner

November 15, 2012

Quicklaw Cite: [2012] B.C.I.P.C.D. No. 23
CanLII Cite: 2012 BCIPC No. 23
Document URL: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF12-04.pdf

TABLE OF CONTENTS

Commissioner's Message

Automated Licence Plate Recognition ("ALPR") technology takes a picture of a vehicle in order to capture its licence plate number. ALPR can be used to enforce traffic bylaws, collect tolls on bridges and roadways, track movements at border crossings, and identify persons of interest to law enforcement. This investigation report focuses on the use of ALPR by municipal police in British Columbia, specifically the Victoria Police Department ("VICPD").

Citizens know little about how police are using ALPR and what happens to their personal information after it has been collected. Further, there are concerns that ALPR could be used as a surveillance tool, where data about the location and activities of law-abiding citizens is stored indefinitely and used for purposes other than that for which it was collected.

These and other concerns were brought to my attention in a written submission made by three individuals that provided a description of police use of ALPR in British Columbia. In light of their submission and the above-noted issues, I commenced a Commissioner-initiated investigation into the use of ALPR by VICPD. I felt it was important to provide citizens with a comprehensive look into how this technology is being used, and also to provide comment on its impact on personal privacy.

The *Freedom of Information and Protection of Privacy Act* ("FIPPA") gives police agencies considerable authority to collect, use and disclose personal information for law enforcement purposes. Technologies like ALPR may be useful in detecting criminal activity, but the volume and type of information collected by police using ALPR, as well as the purpose for collection, must be critically examined and squared with the privacy rights of citizens.

As discussed in this report, I am very concerned about the potential for the retention, and later use and disclosure, of "non-hit" data. This is personal information about the owners of vehicles that are scanned by ALPR, but who are not of interest to police. In recent media reports, law enforcement agencies have openly discussed the possibility of retaining non-hit data. In my view, the use and disclosure of this information for unspecified purposes would not be justifiable under FIPPA. Collecting personal information for law enforcement purposes does not extend to retaining information on the suspicionless activities of citizens just in case it may be useful in the future.

I encourage all public bodies and law enforcement agencies to read this report and its recommendations, which recognizes police authority to use modern technology for law enforcement activities while at the same time respecting the privacy rights of citizens.

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

Executive Summary

The Victoria Police Department ("VICPD") uses Automated Licence Plate Recognition ("ALPR") to scan and record the licence plate number of vehicles and compare them against a list of plate numbers that are of interest to police. In addition to licence plate number, the system also records the time and geographic location of the scan, as well as a photograph of the vehicle and the licence plate.

Modern technologies such as ALPR can be effective law enforcement tools; however, the use of these tools in British Columbia must comply with the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). This automated collection of information raises privacy concerns because, over time, the police could accumulate a large database of information that describes the whereabouts of many individuals, the vast majority of whom were going about routine, lawful daily activities, and thus should be of no interest to police.

I initiated an investigation into the use of ALPR by VICPD to evaluate the privacy risks associated with the use of ALPR by municipal police forces in British Columbia. This report examines whether that use is compliant with FIPPA, and provides guidance for other police forces considering the use of ALPR.

The ALPR program that is used by VICPD is operated in partnership with the Royal Canadian Mounted Police ("RCMP"). The RCMP maintain the primary ALPR database, compile and provide an alert listing to VICPD, and collect information generated by VICPD through its use of ALPR. The alert listing contains a list of licence plates categorized according to the reason for the alert. For example, a licence plate may be listed because it is associated with an unlicenced driver, or because the vehicle was reported stolen.

When a licence plate is scanned and compared against the alert listing, it results in a "hit", a "non-hit", or an "obsolete-hit". A hit occurs when a scanned plate matches a plate number in the alert listing. The ALPR system alerts the officer to the hit, and the officer commences an investigation. A non-hit results when the scanned number does not match a number on the alert listing. An obsolete-hit results where a scanned plate number generates a hit, but the information in the alert listing is out of date and the scanned vehicle is no longer of interest to police.

One of the hit categories in the alert listing is "other pointer vehicle".[1] This category is a composite of sub-categories that while useful to police in other law enforcement contexts, is not relevant to the purpose of ALPR. VICPD is not authorized to collect the personal information associated with this category in the alert listing.

[1] The full contents of this hit category are enumerated in Appendix A of this report.

The report recommends that VICPD work with the RCMP to amend the composition of the other pointer vehicle category to include only that information which is related to the purpose of ALPR.

A key concern is the retention and disclosure of personal information associated with non-hits and obsolete-hits. FIPPA authorizes the collection, use, and disclosure of personal information for a law enforcement purpose. VICPD collects personal information for the purpose of comparison against the alert listing. Once this comparison is accomplished, the authorized use of information associated with non-hits and obsolete-hits has been exhausted. FIPPA does not authorize VICPD to continue to use this information unless it obtains the consent of the individual that the information is about. VICPD is likewise not authorized to disclose this information to the RCMP.

VICPD is required by s. 30 of FIPPA to protect personal information in its custody from, among other things, unauthorized use or disclosure. This requirement precludes VICPD from disclosing non-hit and obsolete-hit information to the RCMP if the personal information will be put to a use that would not be authorized by FIPPA.

A complete list of the findings and recommendations made in this investigation report can be found in Part 3.

1.0 PURPOSE AND SCOPE OF REPORT

1.1 Introduction

This investigation is about the use of Automated Licence Plate Recognition ("ALPR") technology by the Victoria Police Department ("VICPD"). ALPR uses cameras to photograph vehicles in order to identify the licence plate number of the vehicle. VICPD mounts cameras on a patrol car and records the licence plate numbers of vehicles that pass by the car. This information is then compared against a database maintained by the Royal Canadian Mounted Police ("RCMP") which lists licence plate numbers associated with individuals who are of interest to police.

In addition to the licence plate number, the ALPR system records the geographic location where the image was collected, and the time that it was collected. As a result, VICPD creates a record of where and when many drivers in Victoria have been on any given day. Over time, this has the potential to amass a large volume of information about individuals, most of whom are of no interest to police. In this report I examine the collection, use, storage, and disclosure of this information by VICPD.

Advances in technology have enabled the application of novel and increasingly more efficient law enforcement tools by police departments. There is no doubt that many of these tools are useful for detecting criminal activity. However, modern technology also enables the broad and indiscriminate collection of personal information, as well as the retention and processing of large amounts of this information, respecting individuals who are going about their routine, and lawful, business.

The privacy risks associated with modern information technology are potentially significant. The collection and use of personal information have always been a component of government administration, but modern methods enable the collection, retention and manipulation of much larger amounts of personal information, with a corresponding increase in the number of uses to which public bodies can put that information.

The use of potentially privacy-invasive technologies by law enforcement must be balanced against our constitutional right to privacy. As the Supreme Court of Canada has recognized, privacy is essential for individual freedoms, and is of great significance to our communities:

> Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order.

> The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.[2]

The right to choose how much personal information one shares with government, or to know how one's personal information is being used, is fundamental. Moreover, it is a core privacy principle that personal information collected for a purpose should only be used for that purpose. This principle is based on an individual's right to know how their personal information is being used, and by whom. Again, as the Supreme Court has explained:

> In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained.[3]

Once a government has personal information, it may seek to find new uses for that information. This phenomenon, known as 'function creep', is being made increasingly easier as information technology develops newer and more sophisticated means to 'mine' data for useful or interesting patterns, or to link databases of information. For these reasons, privacy laws such as FIPPA seek to protect against function creep by limiting government bodies to collecting only personal information that is necessary for their present programs.

While the collection and use of personal information by police raises a fear in some members of the public, others are unconcerned because they feel they have 'nothing to hide' and are comfortable that those in authority know how to balance privacy rights against the needs of law enforcement. The role of my office is to scrutinize and question the collection, use, and disclosure of personal information by public bodies and organizations, and the security measures in place to protect that information, in accordance with the law.

1.2 Investigative Process

Under s. 42(1)(a) of FIPPA, I have the authority to conduct investigations and audits to ensure compliance with any provision of FIPPA. Section 42(1)(g) further provides me with authority to comment on the privacy implications of automated systems for the collection, storage, analysis or transfer of information.

---

[2] *R. v. Dyment*, 1988 CanLII 10 (SCC), [1988] 2 S.C.R. 417, at para. 17.
[3] *R. v. Dyment*, at para. 22.

On April 27, 2012, I advised Chief Constable Jamie Graham of VICPD that my office had commenced a Commissioner-initiated investigation of VICPD's deployment of ALPR.

On May 25, 2012, investigators from this office conducted a site visit to VICPD, where they were provided with an opportunity to observe how the ALPR system is operated in a traffic patrol vehicle. We were also able to determine what personal information VICPD receives from the RCMP, what personal information is collected by the ALPR system during a VICPD traffic enforcement officer's shift, and what information is subsequently disclosed to the RCMP. Lastly, VICPD demonstrated the security measures that are in place to protect the personal information stored in the ALPR system.

On June 5 and July 10, 2012, my staff met with the Officer in Charge and staff of RCMP "E" Division Traffic Services. On the first visit we inquired into the sources of the RCMP ALPR data, the security of the ALPR database, and the procedures and agreements in place for the use of ALPR by municipal police forces in British Columbia, including VICPD. On the subsequent visit, investigators reviewed the controls surrounding access to the database as well as the types of information stored within the database.

Investigators reviewed a number of documents, including the RCMP's 2009 ALPR privacy impact assessment ("PIA"), VICPD's ALPR use policy, and the agreement in place between VICPD and the RCMP that governs the collection, use, and disclosure of ALPR data between those agencies. They also reviewed PIAs prepared by law enforcement agencies in the United States, and researched the practice for oversight and governance of ALPR in Germany, the United Kingdom, and the United States.

1.3 ALPR in British Columbia

Overview

As noted above, the ALPR system deployed by VICPD consists of a patrol car equipped with specialized cameras and software that record images of vehicles and vehicle licence plates. The system collects the licence plate numbers and then checks them against a list of licence plate numbers that are of interest to the police. When there is a match (a "hit"), the system alerts the officer.

VICPD's ALPR program accesses a database that is maintained by the RCMP. The ALPR program is governed by an agreement ("Participation Agreement")[4]

[4] "E" Division Traffic Services Automatic Licence Plate Recognition (ALPR) Program's Terms and Conditions for Participation, at clause 6 (hereinafter "Participation Agreement").

that describes the relative responsibilities of VICPD and the RCMP. The RCMP is a federal law enforcement agency, and provincial legislation such as FIPPA does not apply to its management or administration.[5] However, a municipal police force is subject to FIPPA and therefore, to the extent that the RCMP ALPR program is used by VICPD, it must meet the requirements of that Act. I will discuss the applicability of FIPPA to ALPR in more detail in Part 1.4 of this report.

History of ALPR

ALPR was initially developed in the United Kingdom as a response to the activities of the Irish Republican Army. It has since been adopted by police and security forces around the world and is currently in use in the United States, Europe, Australia, and elsewhere in Canada.

The usefulness and privacy impacts of ALPR have been questioned by privacy advocates in those countries, and a variety of laws have been passed to restrict or prohibit its use. The Ontario Provincial Police deploy ALPR, and after consultation with the Ontario Information and Privacy Commissioner, configured its system to only retain personal information associated with hits. In New Hampshire, the use of ALPR is only permitted in relation to specific investigations of particular violations, and to provide security for certain designated bridges.[6] In Maine, ALPR is mostly restricted to the protection of transportation infrastructure and law enforcement in relation to "specific articulable facts" regarding public safety or specific criminal investigations, and is not permitted to be used as part of routine law enforcement operations. In addition, Maine limits the retention of ALPR data to 21 days.[7] In Germany, the use of ALPR by police has been examined by the Federal Constitutional Court. That court found that retention of non-hit data was unconstitutional on the ground that it was an encroachment on the fundamental right of informational self-determination.[8]

According to the RCMP, it brought ALPR to British Columbia in response to an increasing number of vehicle thefts. The RCMP had commissioned a study to determine what means were available to assist them in locating stolen vehicles. ALPR was identified as a tool that could be used to rapidly check licence plates and to identify stolen licence plates and vehicles. The ALPR program was then started as a pilot project by the RCMP in 2006, working together with the Government of British Columbia's Ministry of Solicitor General (now the Ministry of Justice) and the Insurance Corporation of British Columbia ("ICBC"), for use by

[5] *Bentley v. Braidwood*, 2009 BCCA 604, at para. 45.
[6] New Hampshire, RSA 261:75-b, *Use of Automated Number Plate Scanning Devices Prohibited*.
[7] Maine, *An Act to regulate the use of automated licence plate recognition systems*; Chapter 605, LD 1561, 124th Maine State Legislature; sets standards for the use of ALPR, and restricts retention of data to 21 days.
[8] BVerfG, BVR 2074/05 of 11.3.2008, Federal Constitutional Court.

the Integrated Municipal Provincial Auto Crime Team.[9] Although ALPR was initially limited to stolen vehicle matters, its scope crept outward. In 2010, the RCMP expanded the program for use by RCMP "E" Division Traffic Services and the province's Integrated Road Safety Unit and began using ALPR as a tool for identifying individuals who were driving while prohibited, unlicenced, or uninsured.

In 2009, media reports suggested that both the Privacy Commissioner of Canada and the then British Columbia Commissioner had approved ALPR as it was deployed at that time. While it is true the RCMP provided both of our offices with a PIA, we in no way approved the project.

ALPR technology and the RCMP database have since been made available to municipal police forces, which access and use the database pursuant to the Participation Agreement with the RCMP.[10] As outlined below, ALPR in the form used by VICPD represents yet another expansion of the 2006 and 2009 uses of ALPR. The RCMP is considering the possibility of retaining non-hit data; were this to occur it would constitute yet another expansion of the program.

The RCMP describes the present goal of ALPR as being "to reduce auto theft and motor vehicle violations in particular those related to prohibited, suspended, unlicenced and uninsured drivers."[11] The 2010 Annual Report of the Road Safety Enhanced Enforcement Program, issued by the Ministry of Public Safety and Solicitor General, described the mandate of ALPR as follows:

> To reduce auto theft and motor vehicle violations related to prohibited, suspended, unlicenced and uninsured drivers. ALPR also assists with recovering stolen vehicles and stolen property, and detecting AMBER[12] Alerts issued for missing children.[13]

How ALPR works

The ALPR system automates a process that would otherwise be undertaken manually by police officers while engaged in routine traffic enforcement. A police officer who is not using ALPR visually identifies a vehicle of interest and enters its licence plate number into a mobile workstation to query the ICBC, Canadian Police Information Centre ("CPIC") and Police Records Information Management

[9] RCMP website, see note 1.
[10] The RCMP currently deploys 41 ALPR-equipped vehicles in British Columbia. Four municipal police departments deploy seven ALPR vehicles: VICPD (1 car), Vancouver Police Department (4 cars), Saanich Police Department (1 car), and Abbotsford Police Department (1 car).
[11] RCMP, "Automatic License Plate Recognition Technology"; http://bc.rcmp.ca/ViewPage.action?siteNodeId=797&languageId=1, accessed July 12, 2012.
[12] America's Missing Broadcast Emergency Response ("AMBER").
[13] 2010 Annual Report, Road Safety Enhanced Enforcement Program, Ministry of Public Safety and Solicitor General, Police Services Division.

Environment[14] ("PRIME") databases. This provides the officer with information related to the licence plate, such as the name of the registered owner, whether that owner has a driver's licence, and whether the vehicle is insured. After evaluating the results, the officer decides whether or not further investigation is warranted.

ALPR automates part of that process; however, there is a significant difference. While a police officer exercises discretion in choosing which vehicles to investigate, the ALPR system photographs and scans every vehicle and licence plate that comes within range of its cameras. My investigators observed VICPD's ALPR vehicle in operation, and were informed by VICPD that it scans an average of 500 vehicles per day of operation, resulting in approximately one hit for every 100 scans.

VICPD's ALPR patrol car is equipped with two forward-facing cameras that photograph vehicles in the passenger-side and driver-side lanes. A third camera is mounted sideways to scan vehicle licence plates in parking lots. The ALPR system uses optical character recognition to convert the licence plate image into text for comparison against the ALPR database alert listings.

When a scanned licence plate matches a plate number in the alert listing, the computer notifies the officer of the hit by sounding an audible alarm and displaying information on the mobile workstation monitor. The images of the vehicle and of the licence plate are displayed along with the category of hit, which indicates why the vehicle is of interest.

To investigate a hit, the officer manually queries the licence plate number on the PRIME, CPIC or ICBC databases using the mobile workstation (in this respect duplicating the manual query process described above). This is the only way the officer is able to access the name of the vehicle's registered owner.

The disposition of a hit will vary depending on the results of this further query. Some alerts do not result in the officer taking any action, either because it is unsafe to pursue the subject vehicle or because the officer determines that the hit warrants no response. For example, what may have been an uninsured vehicle at 6:00 a.m., when the alert listing is loaded into the patrol car's ALPR system, may have been insured by the time it is scanned during the afternoon shift. In such instances, the officer will record through the mobile workstation that the hit did not result in a traffic stop, and will select a disposition category that explains the reason why. When a hit does result in a traffic stop, this disposition is also recorded.

[14] PRIME is a common database shared by all police agencies in the province, including both municipal departments and RCMP detachments. The database records all interaction by individuals with police in British Columbia, including information associated with suspects, witnesses and victims. Municipal forces are required to use PRIME by s. 68.1 of the *Police Act*.

According to VICPD, the ALPR system is not run continuously while the car is on patrol; it is typically used during organised traffic safety projects, which often include other traffic enforcement objectives, such as the enforcement of speed limits, seat-belt use, and hands-free cell phone use.

In general, images captured by the ALPR system do not identify the driver or passengers in the vehicle. The investigators noted that the cameras are directed downward so as to capture the licence plate and the cameras are focussed so that the vehicle or licence plate fills the frame of the image.

By directly observing the scanned images displayed on the patrol car's mobile workstation monitor, we confirmed that, when the front of a vehicle was photographed, an outline of a driver or passenger might be seen, but not with enough detail to enable them to be identified. In some cases, gender might be able to be determined based on hair style or size of the individual.

The RCMP ALPR database

The primary ALPR database is managed and maintained by the RCMP. Municipal police forces within British Columbia are required to sign the Participation Agreement with the RCMP if they wish use the RCMP's ALPR database in their ALPR program. This agreement clearly indicates that the information in the ALPR database is the property of the RCMP and the RCMP is the only body authorized to make changes to the information in the database.

The database contains a list of licence plate numbers categorized according to the reason why their registered owners may be of interest to police. The information is provided to the RCMP by ICBC and CPIC and is updated each morning.

The categories of reasons for licence plates being included in the ALPR database are (with the source agency in brackets):

1. Stolen vehicles (CPIC);
2. Wanted person – Canada Wide (CPIC);
3. Wanted person – BC Wide (CPIC);
4. Prohibited or suspended drivers (ICBC);
5. Uninsured vehicles (ICBC);
6. Unlicenced drivers (ICBC); and
7. Other pointer vehicle (CPIC).

With one exception, these categories are self-explanatory. The 'other pointer vehicle' category is unlike the other hit categories in that it is a composite of many secondary categories of personal information that may be useful for police to know about individuals. For example, this category includes information about individuals who have been refused a firearms certificate, or who may pose a danger to themselves. According to the RCMP, this category is intended to provide contextual information for police regarding an individual who is being investigated. Appendix A lists each of the sub-categories that are contained within this category.

ALPR information flows

Initial collection of the ALPR database from the RCMP

At the beginning of VICPD's traffic enforcement shift, an officer goes to a local RCMP detachment and collects the day's alert listings database for transfer into the ALPR vehicle's mobile workstation. The transfer is done using an encrypted flash drive. The database is automatically erased from the flash drive once it is transferred to the mobile workstation. The officer is not able to decrypt the database, and thus cannot view or change the information on the flash drive. This record is referred to below as the "Alert Listing" record.

End-of-shift disclosure to the RCMP

At the end of a shift the responsible VICPD officer prompts the mobile workstation to initiate the end-of-shift process. This generates a record of that day's ALPR activity, copies that information onto an encrypted flash drive, and deletes it from the mobile workstation. This record consists of images of every scanned licence plate and vehicle, the location and time of each scan and, if the scan resulted in a hit, the disposition of that hit. The officer then returns the flash drive to the local RCMP detachment, where its contents are uploaded to the RCMP ALPR database. This record is referred to below as the "Daily Scans" record.

VICPD also creates a handwritten record of hits that occur during an ALPR shift. This record is retained indefinitely by VICPD. The Participation Agreement requires that a copy of this record be provided to the RCMP. This record is referred to below as the "Handwritten Log".

Anonymization of ALPR information

The images and licence plate numbers of vehicles that did not generate a hit ("non-hits") are automatically deleted from the RCMP ALPR database within 30 minutes after they are uploaded from the VICPD flash drive. The time and location information for non-hits is not deleted from the database. The retention of this information allows the RCMP to track statistics related to the number of

licence plates scanned within a specified timeframe or location without retaining the personal information pertaining to non-hit vehicles.

I will consider whether these instances of collection, use and disclosure are authorized by FIPPA in Part 2 of this report.

1.4 Jurisdiction

Is VICPD a public body?

The definition of terms used in FIPPA is provided in Schedule 1. "Public body" is defined as including a "local government body", which is in turn defined as including "a municipal police board established under section 23 of the *Police Act*". VICPD is governed by the Victoria Police Board and its members are employees of that Board. VICPD is therefore a public body and subject to FIPPA. VICPD's collection, use and disclosure of personal information are regulated by Part 3 of FIPPA.

2.0 ANALYSIS

2.1 Issues Identified

The issues in this investigation are:

1. Does VICPD collect personal information in its use of ALPR? (Schedule 1 of FIPPA)

2. Does VICPD have the authority to collect personal information related to its use of the ALPR system? (s. 26 of FIPPA)

3. Is VICPD required to notify individuals when it collects their personal information? (s. 27(2) of FIPPA)

4. Does VICPD have the authority to use the personal information it collects in relation to its operation of ALPR? (s. 32 of FIPPA)

5. Does VICPD have authority to disclose personal information to the RCMP? (s. 33 of FIPPA)

6. Does VICPD have reasonable security arrangements in place to protect the ALPR-related personal information in its custody? (s. 30 of FIPPA)

2.2 Personal Information

"Personal information" is defined in Schedule 1 of FIPPA as "recorded information about an identifiable individual other than contact information". The first issue is whether VICPD is collecting personal information using ALPR.

ISSUE 1: Does VICPD collect personal information in its use of ALPR?

VICPD collects licence plate numbers and associated information in two instances:

- at the beginning of an ALPR shift, when an officer collects the list of licence plate numbers and hit categories from the RCMP; and
- during an ALPR shift, when an officer collects licence plate numbers from passing cars, the time and geographic location of each scan, and the category of the hit (where applicable).

VICPD has indicated that it does not consider the information collected by ALPR to be personal information. However, the RCMP's PIA for the ALPR program describes licence plates as personal information.

The question of whether a licence plate number is personal information has been considered in several other Canadian jurisdictions. In Investigation Report F2008-IR-002, the Office of the Information and Privacy Commissioner of Alberta found that where a vehicle is owned by an individual (as opposed to a corporation); the licence plate is personal information.[15] That investigation involved the use of ALPR for parking enforcement, and was conducted pursuant to the Alberta *Freedom of Information and Protection of Privacy Act*.

In Ontario, the Information and Privacy Commissioner found that licence plate numbers "are unique identifiers which are assigned to individuals,"[16] and as such are personal information pursuant to the *Municipal Freedom of Information and Protection of Privacy Act*. Further, in an investigation report issued in 2003 regarding Toronto police use of ALPR to find stolen vehicles, the Ontario Information and Privacy Commissioner accepted that a licence plate number is personal information.[17] The definition of personal information in both the Alberta and Ontario Acts is for present purposes the same as the definition in FIPPA.

[15] [2008] A.I.P.C.D. No. 76, at para. 26.
[16] Order M-336, [1994] O.I.P.C. No. 200, at para. 5.
[17] http://ipc.on.ca/images/Findings/up-mc_030023_1.pdf.

This office has previously held that information is "about an identifiable individual" if information can be linked to individuals through other available information.[18] Other Canadian Commissioners have taken the same approach, as have Canadian courts.[19]

The Alberta Court of Appeal has recently addressed a similar question, albeit in the different context of Alberta's private sector privacy law. In *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*,[20] a majority of the Court decided that licence plate numbers were not personal information under the Alberta *Personal Information Protection Act*. A furniture store was collecting the licence plate numbers of individuals who picked up furniture in its loading dock. The purpose of the collection was to prevent fraud by maintaining a record that could be used if the wrong person picked up a piece of furniture.

Although *Leon's Furniture* is not binding on me, it merits consideration. The majority held that a licence plate number is tied to a vehicle, not an individual, so it is "about" the vehicle, not the individual. The majority accepted that a licence plate "may well be connected to a database that contains other personal information, but … the appellant [the store] had no access to that database, and did not insist that the customer provide access to it."[21] I also note that the majority acknowledged that it would not be "determinative" if a licence plate number were connected to a database that "contains other personal information", from which I infer that such a linkage might, in the majority's view, be a factor in determining whether a licence plate number is personal information.[22]

The use of licence plate numbers by VICPD is very different from that in *Leon's Furniture*. Police have routine operational access to the motor vehicle registry database maintained by ICBC, and use licence plate numbers precisely because they link to personal information about individuals, in the ICBC database, the ALPR database, CPIC and PRIME. In other words, the very reason police collect licence plate numbers is to gain access to recorded information about identifiable individuals. This is consistent with the reasons of Conrad J.A. in her strong, and persuasive, dissent in *Leon's Furniture*, noting, among other things, that a licence

---

[18] Order 04-06, [2004] B.C.I.P.C.D. No. 6.
[19] See, for example, *Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner)*, 2001 CanLII 32755 (ON SCDC), (aff'd *Ontario (Attorney General) v. Pascoe*, 2002 CanLII 30891 (ON CA), (2002). The court held in that case that any information which, when combined with other information, could identify a person, qualified as information about an identifiable individual. Also see *University of Alberta v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 112.
[20] 2011 ABCA 94, leave to appeal to the Supreme Court of Canada denied November 24, 2011, 2011 CanLII 75277 (SCC).
[21] *Leon's Furniture*, para. 49.
[22] *Leon's Furniture*, para. 49.

plate number is "merely a conduit" to personal information that is not publicly available.[23]

The information collected by VICPD from the RCMP in the Alert Listing record consists of a list of licence plate numbers and corresponding hit categories that apply to each plate number. A VICPD officer is easily able to link the licence plate number to the identity of the registered owner by accessing the CPIC, ICBC, and PRIME databases. This is a routine procedure for a police officer, and this ability to link the plate number to a specific individual is the very reason for the use of the plate number as an identifier in the Alert Listing record. This discloses information explaining to the officer why that person is of interest to police. Because of this ability to readily and routinely link a licence plate number to an individual, and to information about that individual, the licence plate number is personal information.

During an ALPR shift, while the ALPR system is operational and the cameras are activated, VICPD is collecting images of licence plates and vehicles, information about the time and geographic location of each image, whether the scan resulted in a hit, and the disposition of that hit. Information generated respecting the time and location of a scan, and the disposition of a hit, is information about an individual. This, too, is personal information. The information is about the registered owner in that it places her or his vehicle in a certain place at a certain time. Therefore, both information collected in the Alert Listing, and information captured and generated by the ALPR system and recorded in the Daily Scans record, is personal information.

I find that the licence plate and associated information collected, used, and disclosed by VIPCD in its operation of ALPR is personal information as defined by Schedule 1 of FIPPA.

2.3 Collection of Personal Information

A public body must have authority under FIPPA for the collection of personal information. Section 26(b) of FIPPA authorizes the collection of personal information for the purposes of law enforcement. "Law enforcement" is defined in Schedule 1 of FIPPA as:

> (a) policing, including criminal intelligence operations,
>
> (b) investigations that lead or could lead to a penalty or sanction being imposed, or
>
> (c) proceedings that lead or could lead to a penalty or sanction being imposed.

[23] *Leon's Furniture*, para. 121.

ISSUE 2: Does VICPD have the authority to collect personal information related to its use of the ALPR system?

VICPD stated that at present it is using the ALPR system primarily as a traffic enforcement tool. It does this by identifying vehicles owned by individuals who are unlicenced, uninsured, or driving while prohibited. These specific purposes for collection qualify as law enforcement purposes.

Again, VICPD collects the following information through its use of ALPR:

- licence plate number and hit category in the Alert Listing record collected from the RCMP; and
- licence plate number, licence plate and vehicle images, and geographic location and time for all vehicles scanned by the ALPR system during an officer's shift, all of which is collected, compiled and recorded in the Daily Scans record.

Collection of information in the Alert Listing record

The Alert Listing record is collected by VICPD from the RCMP and uploaded into the patrol car's mobile workstation. This record is composed of the hit categories listed in Part 1.3 of this report. With the exception of the other pointer vehicle category, the collection by VICPD of the information contained in each of these categories is serving a law enforcement purpose. For example, when the ALPR system alerts a VICPD officer of an uninsured vehicle or of an unlicenced driver, the officer is provided with information that is relevant to the purposes for ALPR.

However, the other pointer vehicle category is a composite category, consisting of eleven sub-categories, most of which are only useful to provide contextual information to an investigation but not sufficient in themselves to initiate an investigation. While this information is likely useful in ordinary police operations, its broad scope is not well-adapted to use as an ALPR hit category because much of the information is not relevant to the activity of an officer while using ALPR. For example, it is not serving a law enforcement purpose for a VICPD officer to be alerted when the ALPR system scans a vehicle whose owner once attempted suicide. I understand that this information is valuable to police in other contexts. It is certainly relevant to an officer that an individual has a history of violence or of attempting suicide while in police custody. However, it is not relevant for the ALPR system to alert the officer that such a person has just driven past the patrol car.

While each of the other pointer vehicle sub-categories may serve a valid law enforcement purpose in other circumstances, in the context of ALPR many of them are not useful, and there is no law enforcement rationale for the collection

of this information. There are, however, sub-categories within the other pointer vehicle category that are relevant to ALPR. For example, it is relevant that an individual is prohibited by court order from driving a vehicle. The difficulty presented by the other pointer vehicle category is that it contains both relevant and irrelevant sub-categories. As it is currently configured, the ALPR system does not allow VICPD to selectively collect only those sub-categories that are relevant to ALPR; the other pointer vehicle can only be collected in its entirety.

I find that collection by VICPD of the information contained in the RCMP Alert Listing record, except for that information contained in the other pointer vehicle category, is authorized by s. 26 (b) of FIPPA as being for the purposes of law enforcement.

I find that collection by VICPD of the other pointer vehicle category as it is presently constituted in the Alert Listing record is not authorized by FIPPA.

RECOMMENDATION 1:

I recommend that VICPD work with the RCMP to amend the composition of the other pointer vehicle category to include only that information which is related to the purpose of ALPR.

Collection of information in the Daily Scans record

VICPD collects an image of the vehicle and licence plate, the licence plate number, geographic location, and time of scan for each vehicle. The collection of the licence plate number is necessary to facilitate the comparison with the Alert Listing record. The image of the vehicle and licence plate enables the officer to check that the ALPR software has correctly read the plate number from the image. This collection is for the law enforcement purpose of identifying those scanned cars that are listed in the Alert Listing record.

I find that collection of licence plate number, licence plate and vehicle image, geographic location, and time of scan for all vehicles scanned by the ALPR system is authorized by s. 26(b) of FIPPA as being for a law enforcement purpose.

2.3.1 Indirect Collection of Personal Information

Under FIPPA, the general rule is that information must be collected directly from the individual that the information is about. However, s. 27(1)(c)(iv) of FIPPA authorizes the indirect collection of personal information for the purpose of law enforcement.

The collection of personal information by VICPD from the RCMP that relates to hits is for a law enforcement purpose. Therefore pursuant to s. 27(1)(c)(iv) of FIPPA, VICPD is authorized to indirectly collect personal information for ALPR.

2.4 Notification

FIPPA requires a public body that collects personal information to inform the individual the information is about of the purpose for collecting it, the legal authority for collecting it, and the contact information of an official or employee of the public body who can answer questions about the collection.[24]

ISSUE 3: Is VICPD required to notify individuals when it collects their personal information?

Section 27(3) of FIPPA provides that notice is not required if the information is about law enforcement. I find that, because the collection of personal information by VICPD through the use of ALPR is for a law enforcement purpose, VICPD is not required to notify individuals of the collection of their personal information.

2.4.1 Transparency of the Mandate of ALPR

The RCMP and the Ministry of Justice publish information about the ALPR program that describes the mandate of the program. This information describes the mandate as relating to auto theft, traffic enforcement, and the detection of missing children through the AMBER Alert program. Neither the Ministry nor the RCMP mentions that ALPR is also used to identify wanted persons or individuals in any of the sub-categories in the other pointer vehicle category.

An accurate description of the program mandate would provide for greater public transparency, facilitating public accountability for the collection and use of personal information through ALPR. The public should be informed of the full scope of ALPR.

[24] The content of the notification requirement is enumerated in s. 27(2) of FIPPA.

RECOMMENDATION 2:

I recommend that the mandate of ALPR be more accurately described by VICPD and the Ministry of Justice to inform the public of the full scope of the ALPR program.

2.5 Use of Personal Information

Section 32 of FIPPA authorizes a public body to use personal information for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose.

One of the most common privacy risks occurs when personal information collected by a public body for one purpose is subsequently used for a different purpose. Section 32 of FIPPA therefore sets limits for public bodies by clearly stating the purposes for which personal information in their custody or control may be used, and limiting other uses to consistent uses.

ISSUE 4: Does VICPD have the authority to use the personal information it collects in relation to its operation of ALPR?

I have already found that VICPD collects personal information for a law enforcement purpose. Therefore, to the extent I have found VICPD is authorized to collect personal information, the use of this personal information for that purpose is authorized by s. 32(a).[25]

VICPD uses the collected licence plate and vehicle images, geographic location and time of the scan, and hit category to facilitate the comparison of scanned licence plate numbers against those listed in the Alert Listing record. This law enforcement use is the purpose for which it was originally obtained.

I find the use of personal information contained in the ALPR records by VICPD is authorized by s. 32(a) of FIPPA as being for the purpose for which it was obtained or compiled.

2.6 Disclosure of Personal Information

Section 33 of FIPPA requires a public body to ensure that personal information in its custody or under its control is disclosed only in accordance with ss. 33.1, 33.2,

[25] As I have found that VICPD is not authorized to collect the other pointer vehicle category in the Alert Record, the use of that category is also not authorized.

or 33.3. Section 33.1(2) of FIPPA allows a public body that is a law enforcement agency to disclose personal information to another law enforcement agency in Canada.

ISSUE 5: Is VICPD authorized by FIPPA to disclose personal information to the RCMP?

2.6.1 VICPD's Disclosure of ALPR Hit Data

VICPD discloses the Daily Scans record to the RCMP. This record contains the personal information for every registered owner of a vehicle that is scanned by the ALPR system.

Section 33.1(2)(a) authorizes the disclosure of personal information by VICPD to another law enforcement agency in Canada. FIPPA does not expressly require that this disclosure between law enforcement agencies be for a law enforcement purpose, but I have no doubt this is what the Legislature intended. This interpretation is harmonious with the scheme of FIPPA, its object, and the intention of the Legislature.[26]

In any case, both VICPD and the RCMP are law enforcement agencies and the disclosure of personal information associated with hits is for a law enforcement purpose.

I find that the disclosure of personal information associated with hits by VICPD to the RCMP is authorized by s. 33.1(2) as being disclosure between two law enforcement agencies, for a law enforcement purpose.

2.6.2 VICPD's Disclosure of ALPR Non-hit Data

The initial use of scanned licence plate numbers for comparison against the Alert Listing record is a law enforcement use that is authorized by FIPPA. However, information that resulted in non-hits is information about the law-abiding activities of individuals that the police have no reason to believe relates to criminal activity, and is thus no longer serving a law enforcement purpose.

The information relating to non-hits ceased to be associated with a law enforcement purpose once the ALPR system determined that the licence plate number did not match a number on the Alert Listing record. Therefore, the disclosure of non-hit personal information by VICPD to the RCMP is not

[26] E. A. Driedger, *Construction of Statutes* (2nd ed. 1983), at p. 87, as cited in *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27, at para. 21; see also *Bell ExpressVu Limited Partnership v. Rex*, [2002] 2 S.C.R. 559, 2002 SCC 42, at para. 26.

authorized by FIPPA because that information is no longer serving a law enforcement purpose.

The Participation Agreement entered into between the RCMP and VICPD stipulates that "ALPR images and data related to non-hits are not retained." As noted earlier, my investigators have confirmed that the personal information associated with non-hits is de-identified after it is disclosed to the RCMP. Vehicle and licence plate images are deleted immediately as they are uploaded to the RCMP ALPR database. The licence plate number and licence plate image are automatically deleted within 30 minutes of being uploaded. At that point the non-hit information is de-identified and ceases to be personal information.

VICPD takes the position that it does not disclose any non-hit information to the RCMP. However, the personal information related to non-hits that is contained in the Daily Scans record is in the custody of VICPD prior to being uploaded into the RCMP database. A VICPD officer discloses this information to the RCMP at the end of the ALPR shift, and the RCMP would not have access to this information were it not for this disclosure. This is an unauthorised disclosure of personal information by VICPD to the RCMP.

I find that disclosure of non-hit personal information by VICPD to the RCMP is not for a law enforcement purpose, and is therefore not authorized by FIPPA.

RECOMMENDATION 3:

I recommend that the ALPR system be configured to delete personal information associated with non-hits immediately after the system determines it does not match a licence plate number in the Alert Listing.

2.6.3 Obsolete-hits

An obsolete-hit occurs when the ALPR system indicates a licence plate number is associated with a hit category, but the hit category no longer applies to that vehicle. This is not unusual when, for example, a vehicle is uninsured at the time the database is updated in the morning, but between that time and the time the vehicle is scanned the owner has insured the vehicle. This type of obsolete-hit does not result in a traffic stop because when the VICPD officer queries the CPIC, ICBC and PRIME databases to investigate the hit, the updated insurance information is provided. An obsolete-hit is classified by the ALPR system as a hit in the Daily Scans record.

We were informed that approximately four per cent of hits are obsolete-hits, and over time the retention of this obsolete-hit information results in the retention of a significant amount of personal information that is not necessary for any ongoing law enforcement purpose.

RECOMMENDATION 4:

I recommend that the ALPR system be configured to delete personal information associated with obsolete-hits immediately after the VICPD officer determines that no further investigation of the vehicle is warranted.

2.7 Protection of Personal Information

Section 30 of FIPPA requires public bodies to take reasonable security measures to protect personal information from unauthorized access. Section 30 states:

> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

ISSUE 6: Does VICPD have reasonable security arrangements in place to protect the personal information used for ALPR?

2.7.1 Protection Against Unauthorized Access

The information within the ALPR database is protected at a number of levels. The RCMP ALPR database is held within the RCMP's networks. Investigators from my office audited the technical security of that database and determined it to be highly secure. Only two individuals have access to the database, for viewing or maintenance purposes. When requests are received related to law enforcement proceedings, they must be authorized by the Superintendent of RCMP "E" Division, who reviews each request to ensure it is related to an investigation. Approximately 12 of these requests are received each year in British Columbia.

The VICPD police officers operating the ALPR system do not have access to the RCMP database itself. The Alert Listing and Daily Scans records are encrypted while on the flash drive. The decryption of the Alert Listing is done by software

within the mobile workstation's processing unit in the police vehicle. Police officers are prohibited by policy from adding licence plate numbers to the Alert Listing except in the case where an AMBER alert is issued. This policy is in place to protect the integrity of the database. The database administrator is able to identify any plates manually entered into the system and to confirm that they are related to an AMBER alert.

I find that VICPD has made reasonable security arrangements to protect personal information associated with the ALPR program against such risks as unauthorized access, collection, use, disclosure or disposal pursuant to s. 30 of FIPPA.

2.7.2 Protection Against Subsequent Use of Non-hit Data

The information in the Daily Scans record is the product of the activities of a VICPD officer while acting in the course of his or her duties, and the content of this record relates directly to the mandate and functions of VICPD. Where a record is created by a public body as part of its mandate and functions, it is generally considered to be within its custody and under its control.[27]

VICPD has custody of the non-hit information that is recorded in the Daily Scans record, and is required to take reasonable measures to protect this data from, among other things, unauthorized use. The personal information contained in the Daily Scans record that relates to non-hits has already been used for the law enforcement purpose for which it was originally collected, and that use has been exhausted. Consequently, VICPD finds itself in control of volumes of personal information that it cannot use for another purpose without the consent of the individuals that the information is about.

Reasonable measures to protect against unauthorized use, in my view, would include denying access to the non-hit data by any organisation that has indicated the information will be used for a purpose that would not be authorized by FIPPA.

The RCMP has stated that it is considering changing the ALPR program such that non-hit personal information would be retained on the ALPR server. I have already determined that the disclosure of non-hit information by VICPD to the RCMP is not authorized by FIPPA. I note here that s. 30 of FIPPA would also prohibit VICPD from disclosing this information to the RCMP. VICPD cannot disclose that information knowing it will be used in a manner not authorized by FIPPA without failing to meet its obligation to take reasonable security measures against unauthorized use.

[27] Order 04-19, [2004] B.C.I.P.C.D. No. 19, at para. 46.

3.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

3.1 Summary of Findings

I have made the following findings in this investigation:

The licence plate information collected, used, and disclosed by VIPCD in its operation of ALPR is personal information as defined by Schedule 1 of FIPPA.

The collection by VICPD of the information contained in the RCMP Alert Listing record, except for that information contained in the other pointer vehicle category, is authorized by s. 26(b) of FIPPA as being for the purposes of law enforcement.

The collection by VICPD of the other pointer vehicle category in the Alert Listing record is not authorized by FIPPA.

The collection by VICPD of licence plate number, licence plate and vehicle image, geographic location, and time of the scan for all vehicles scanned by the ALPR system is authorized by s. 26(b) of FIPPA as being for a law enforcement purpose.

The use of personal information contained in the ALPR records by VICPD is authorized by s. 32(a) of FIPPA as being for the purpose for which it was obtained or compiled.

The disclosure of personal information associated with hits by VICPD to the RCMP is authorized by s. 33.1(2) as being disclosure between two law enforcement agencies, for a law enforcement purpose.

The disclosure of non-hit personal information by VICPD to the RCMP is not for a law enforcement purpose, and is therefore not authorized by FIPPA.

VICPD has made reasonable security arrangements to protect personal information associated with the ALPR program against such risks as unauthorized access, collection, use, disclosure or disposal pursuant to s. 30 of FIPPA.

3.2 Summary of Recommendations

RECOMMENDATION 1

I recommend that VICPD work with the RCMP to amend the composition of the other pointer vehicle category to include only that information which is related to the purpose of ALPR.

RECOMMENDATION 2

I recommend that the mandate of ALPR be more accurately described by VICPD and the Ministry of Justice to inform the public of the full scope of the ALPR program.

RECOMMENDATION 3

I recommend that the ALPR system be configured to delete personal information associated with non-hits immediately after the system determines it does not match a licence plate number in the Alert Listing.

RECOMMENDATION 4

I recommend that the ALPR system be configured to delete personal information associated with obsolete-hits immediately after the VICPD officer determines that no further investigation of the vehicle is warranted.

4.0 CONCLUSIONS

ALPR automates a process that would otherwise be conducted manually by a VICPD police officer. This distinction between the product of the manual process versus the automated process is a key aspect of the use of ALPR as a law enforcement tool; information is collected without exercising any judgement regarding the need for collection. The unfortunate side-effect of this automation is the creation of a large record containing personal information that is not related to a hit, and is therefore not of interest to police.

VICPD collects personal information from the RCMP in the form of the Alert Listing. With the exception of the other pointer vehicle category, this record contains information that is relevant to the operation of ALPR, and its collection is

authorized by FIPPA as being for a law enforcement purpose. However, the collection of data from the other pointer vehicle category, as it is presently constituted, is not authorized by FIPPA. I recommend that the other pointer vehicle category be amended to include only those sub-categories that are related to the purpose of ALPR.

When a scanned vehicle licence plate is compared against the Alert Listing and results in either a non-hit or an obsolete-hit, the law enforcement purpose for the use of that personal information is exhausted. Subsequent use by VICPD of personal information associated with non-hits or obsolete-hits is not authorized by FIPPA without the consent of the individual the information is about.

VICPD currently discloses non-hit information to the RCMP. This information is de-identified by the RCMP within 30 minutes of the disclosure. The intention of this de-identification is to prevent the retention of non-hit personal information. However, there is nevertheless a disclosure by VICPD to the RCMP. This disclosure of non-hit information is not serving a law enforcement purpose, and is not authorized by FIPPA.

The RCMP has indicated to my office and to the media that it is considering changing the ALPR program such that non-hit information would be retained. The retention and subsequent use of non-hit and obsolete-hit personal information would result in the creation of an expansive database that describes the whereabouts of many British Columbians as they go about their routine daily activities. I do not have jurisdiction to direct the RCMP in their use of ALPR, however, I am nevertheless deeply concerned about the potential privacy implications of this indiscriminate collection of personal information.

ALPR is a useful tool, enabling VICPD to efficiently accomplish legitimate law enforcement objectives. However, as the complicated issue of non-hit and obsolete-hit information illustrates, the indiscriminate nature of this automated collection of personal information is extremely problematic. It is important that we routinely evaluate and address the threats to privacy posed by new technologies such as ALPR. This will enable the development of best practices that respect personal privacy, and will ensure that the use of the technology is compliant with privacy legislation.

I encourage municipal police departments that are considering the use of ALPR to consider the findings and recommendations in this report to facilitate the design of an ALPR program that is compliant with FIPPA and respectful of the privacy interests of British Columbians.

5.0 ACKNOWLEDGEMENTS

Victoria Police Department and the RCMP “E” Division cooperated fully with our investigation.

Patrick Egan, Senior Investigator, and Bradley Weldon, Policy Analyst, conducted this investigation and assisted in preparing this report.

November 15, 2012

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

Appendix A

Other pointer vehicle

The components of the other pointer vehicle category are:

i. Accused person;
   - a person against whom legal proceedings have commenced;

ii. Court action;
   - a person who has legal custody of a child as specified in an order of the court; or
   - a person against whom proceedings have commenced and who:
     - has been released pursuant to a suspended sentence, conditional sentence, probation, peace bond or other interim measure;
     - is a person whose case has been resolved by alternative measures under the *Criminal Code* or the *Youth Criminal Justice Act*; or
     - is a person who has been found not guilty by reason that they were Not Criminally Responsible on account of Mental Disorder ("NCRMD"), and are subject to release conditions;

iii. Firearms interest police;
   - a person involved in an incident as described in s. 5 of the *Firearms Act* of Canada

iv. Missing person;

v. Parolee;

vi. Prohibited person;
   - a person against whom an Order of Prohibition is in effect with regard to liquor, firearms, vehicle driving (and boat operation), hunting or any other court or statute-imposed prohibition;

vii. Refused person;
   - a person who has been refused a firearms licence or certificate pursuant to the *Criminal Code* or the *Firearms Act*;

viii. Special interest police;

- A person who is known to:
  - be dangerous to police, himself/herself or other persons;
  - have threatened or attempted suicide either when in or out of police custody;
  - be a foreign fugitive but no warrant is available or the fugitive is not arrestable in Canada;
  - be in danger of family violence;
  - be involved in or committing criminal offences;
  - be overdue on a weekend or day pass from a federal penitentiary;
  - be a high risk for future violent conduct;
  - have been absolutely discharged by a Review Board, having previously been found not guilty by reason of being NCRMD

ix. Known associate;

- the next-of-kin or known associates of the subject of a primary CPIC record

x. Pointer person;

- this secondary category is used to record data on a person linked to a primary record, *i.e.* property, vehicle, etc. This category is used to "point" to the record of primary interest.

xi. Surveillance person;

- a person suspected of committing criminal offences;
- a person involved in a serious criminal investigation and information regarding his or her whereabouts is required;
- persons are recorded in this category so that their movements will be monitored not only by the originating agency but also by any agency making a query on the record. The agency making the query must inform the originating agency of the circumstances involving the person.