Automatic Number Plate Recognition

Table of Contents

Overview

ANPR

Automatic Number Plate Recognition (ANPR) is a technology used to automatically read motor vehicle number plates by use of optical character recognition (OCR). The data obtained is referred to as Number Plate Information (NPI). NPI can come from a fixed ANPR camera or a mobile ANPR camera. NPI may also be collected by running OCR over CCTV footage that does not have built in ANPR capability, providing the CCTV footage is of readable quality.

ANPR cameras will capture NPI for every vehicle that has a number plate that can be read, logging a date and time stamp. This data is able to be automatically compared against Vehicles of Interest (VOI) in various databases including Police's National Intelligence Application (NIA), Waka Kotahi 's Motor Vehicle Register (MVR) and Driver Licence Register (DLR).

When a VOI is identified, a system alert is generated. An operator monitoring any alerts can conduct a TENR Threat assessment to determine an appropriate response e.g., the detection of a stolen vehicle.

NPI data that is captured may be retained and stored in line with Police and private companies own policies so that it can be reviewed for VOIs in relation to historical offences.

ANPR Sources

Police currently has access to NPI from three main sources:

1. Police owned and operated ANPR cameras. These are primarily mobile cameras that can be deployed in vehicles, although a small number of static cameras exist.

For safe operational deployment procedure of ANPR in vehicles refer to ANPR Vehicle Operating Procedures (SOP)

2. ANPR cameras owned and operated by other government agencies, such as Waka Kotahi and local authorities (e.g., City Councils).

3. Third party operators that provide Police access to NPI data from private companies that own and operate ANPR networks.

Refer to Requests for Information of Number Plate Information (NPI) from Automatic Number Plate Recognition Technology (SOP)

Police use of ANPR

Police uses ANPR technology and the NPI it provides for a range of enforcement, staff safety and public safety purposes:

Use of real-time (or as near real time as possible) ANPR data for crime prevention, staff safety and immediate response activities as follows:

- Police can deploy
    - ANPR equipped patrol vehicles to locations of interest for targeting all VOI subsets in the Police National Intelligence application (NIA)
    - ANPR equipped patrol vehicles to identify vehicles that have flags in NIA indicating that person(s) associated to the vehicle pose a risk to staff safety. This enables Police to take appropriate steps to mitigate any risk to staff prior to stopping a vehicle
    - to vehicles with a 'stolen' alert identified by third party ANPR networks
- Police can also provide specific vehicle NPI details to third party operated ANPR networks in cases where there is a reasonable belief a risk to life or safety of any person or a serious threat to public health or public safety exists, Police have a warrant authorising tracking of a person or vehicle, or where Police invoke urgency or emergency provisions of section 48 of the Search and Surveillance Act that permit tracking of a person or vehicle.
- This provides an opportunity to deploy to any alerts identified.

Use of retained (i.e., historical) NPI for investigative, evidentiary and intelligence purposes for the investigation of offences including:

- Investigate offences involving the use of motor vehicles after the offence has taken place. Specifically, to obtain location and time stamp data on VOIs suspected of being used in the commission of offences. NPI can assist in providing relevant evidence as part of a prosecution for the offence involving or linked to a particular VOI.
- Investigate an offence after it has taken place that is suspected to have been committed by a person who owns and/or uses a VOI. Specifically, to obtain location and time stamp data on VOI listed as being owned or used by a person being investigated for the commission of an offence. NPI can assist in establishing the location of VOI (and persons associated to that VOI) which can assist in providing relevant and valuable evidence of a suspect's involvement in the offence under investigation.
- Intelligence gathering in respect of any vehicle linked to a person under investigation for an offence or a vehicle linked to an offence or offences under investigation for which a suspect has not been identified. NPI can provide relevant intelligence as to locations of such vehicles at relevant times. This enables analysis and identification of any vehicle behaviour patterns which can assist in preventing further offending, gathering evidence of offending and identifying suspects.

We protect our people, our information, & our resources

We need to consistently practice good judgement and integrity when creating, accessing, modifying and using, securing and disclosing all ANPR generated information. We always need to handle such information appropriately, for legitimate work purposes and in line with the law, this policy and associated processes and systems.

Access to ANPR generated information is only permitted in accordance with this Policy and accompanying Standard Operating Procedures (SOPs).

Use of ANPR generated information outside this policy may be considered unauthorised use and subject to an employment investigation which could lead to disciplinary action.

ANPR Policy

When an ANPR camera is deployed, it will capture NPI of every vehicle that is readable by the camera. NPI data falls under the definition of personal information under the Privacy Act 2020, particularly when it is linked up to a database that connects a number plate to the owner of the vehicle and must be managed accordingly.

The vast majority of NPI is of no interest to Police as it will not be matched to a VOI. Even so, it is data collected about individuals that requires appropriate secure storage, access restrictions and deletion of data in a timeframe commensurate with the purposes of its use.

This document sets out Policy principles for:

- collection, retention, use and disposal of Police owned NPI
- Police use of NPI collected by third party operators
- guidance and examples of approved ANPR use
- Governance and Assurance Reporting model.

Use of Police owned and generated NPI data

Police collects NPI to link vehicles to offenders and offences.

Law enforcement Purpose

Police own and operate mobile ANPR cameras and static ANPR cameras.

Police collect vehicle information including NPI, make, model and colour etc. while recording incidents in NIA. Where someone is known or suspected to have committed an offence, the MVR can be checked to identify vehicles registered to that person. Any vehicle reported as involved in an offence can also be checked against the MVR, so that the owner may be contacted regarding investigations into the offending.

NPI is only of interest to Police in relation to investigations of known or suspected offending. Police collect NPI so it can be matched to known vehicles of interest (VOI) to enhance real time detection and apprehension opportunities. This includes for example stolen vehicles, vehicles linked to a life threatening or otherwise serious incidents, and vehicles that are linked to persons who are the subject of a warrant to arrest or are wanted to arrest for an offence. Any vehicle that has a VOI alert in NIA that is captured by Police ANPR (both fixed and mobile) will trigger an alert giving an opportunity for Police to respond.

Real time response relies on VOI alerts entered into NIA, to which NPI is matched

All VOI identified in NIA, as with all other NIA data, requires appropriate access permissions, including that the data can only be accessed by Police staff for legitimate work purposes.

District intelligence units and operational groups are authorised to create NIA alerts, by linking high risk drivers or offenders to vehicles, to target specific risks they create. This provides a mechanism for matching NPI to VOI's to generate alerts in real time and provide location evidence for intelligence profiling and investigative purposes in historical time.

For the subset of VOI alerts that form part of the VOI extract file exported daily for download to Police ANPR units as the basis for ANPR 'hits', expiry dates are critical to effective use of ANPR and mobile queries. VOI alerts that could trigger a real-time response must be kept up to date. It is important to clear VOI alerts when they are no longer active e.g., stolen vehicle recovered; offender apprehended etc. As a default, an appropriate expiry date for VOI alerts should be entered at the time the entry is made.

Where a VOI is entered into an ANPR extract file, there must be a clear understanding of Police's lawful authority to stop the vehicle should it be detected. The only VOI alert codes to be used, which are included in the ANPR VOI extract file in the Back Office System Software (BOSS) system for real time response are those that correspond to a legislative power to stop a vehicle. Those codes are set out in the table below:

VOI Alert	Power to Stop Vehicle
Warrant to arrest	S9 Search and Surveillance Act 2012
Wanted to interview sufficient for arrest	S9 Search and Surveillance Act 2012
Known to be driven by a disqualified driver	S114 Land Transport Act
Known to be driven under the influence of Drugs or Alcohol	S114 Land Transport Act
Driver Forbidden to Drive	S114 Land Transport Act
Non-Op Order - Pink Sticker	S114 Land Transport Act
Non-Op Order - Green Sticker	S114 Land Transport Act
Prohibition Notice s.248 LTA issued Wrecked - i.e., plates removed from vehicle for disposal	S114 Land Transport Act
Stolen vehicle alert	S9 Search & Surveillance Act
Petrol Drive Off	S9 Search & Surveillance Act (provided reasonable grounds to believe a person in the vehicle has committed an offence punishable by imprisonment)
Other (specify - boy racer events)	Intelligence only - no power to stop vehicle unless section 114 of the Land Transport Act or section 9 of the Search & Surveillance Act provision apply
Person Safety Alert	Intelligence only - no power to stop vehicle unless section 114 of the Land Transport Act or section 9 of the Search & Surveillance Act provision apply
Organisation Safety Alert	Intelligence only - no power to stop vehicle unless section 114 of the Land Transport Act or section 9 of the Search & Surveillance Act provision apply
Sought	Intelligence only - no power to stop vehicle unless section 114 of the Land Transport Act or sections 9 or 121 of the Search & Surveillance Act provision apply
Important Information.	Intelligence only - no power to stop vehicle unless section 114 of the Land Transport Act or sections 9 or 121 of the Search & Surveillance Act provision apply

Retention of Police NPI data must be linked to a specific purpose

Police may retain Police generated NPI for a period of 12 months to enhance investigative and detection opportunities in respect of vehicles that become of interest to offences under investigation after the NPI data has been captured. These vehicles will not be flagged as a VOI at the time they are captured by the ANPR camera and therefore will not have triggered an alert.

Delays in offences being reported and the identification of persons and vehicles of interest to investigations is an evolving process that can develop over weeks or months. The retention of NPI can enhance investigation outcomes by providing a means for Police to be able to identify specific locations of vehicles of interest over a defined period. It may also be accessed by intelligence staff compiling evidence about a known offender's movements in a specific vehicle in relation to involvement in serious or organised crime.

The ability to conduct a retrospective review of retained NPI both on Police and third party stored NPI databases will have two primary applications:

1. The investigation of offences.
2. The potential ability to conduct intelligence analysis that can build a "pattern of life" picture of a particular vehicle(s) movements over a period of up to 12 months.

Investigation of offences

Where an investigation is being conducted into an offence and a particular vehicle is connected in any way to that offence, a retrospective review of NPI in relation to that vehicle can be conducted in accordance with the access and approvals section of this policy and accompanying SOPs.

Any relevant NPI becomes evidential material in relation to that investigation and can be introduced onto the investigation file as a permanent record. This applies both to cases where a vehicle registration number is already known to Police or where Police uses ANPR/CCTV to identify a vehicle registration number from a vehicle description.

Intelligence reviews

The collection and retention of NPI data for a period of 12 months allows the movements of a particular vehicle to be analysed to build up a picture of the regular movements of that vehicle. There is potential to predict with a high degree of accuracy where a particular vehicle is likely to be at a certain day and time as well as link a vehicle to specific locations of relevance to an offence under investigation.

Storage, access, and review of retained Police NPI data

Storage, access, and review of such information may generally be considered to be an intrusion of privacy and can only be justified if the law enforcement purpose for conducting this analysis outweighs the right to privacy.

Police owned and generated NPI data may be retained and stored for up to 12 months.

Access and review of that data is for legitimate work-related purposes only and must be in accordance with the access and approvals process outlined in the following table.

Data Access for Offences		
Period elapsed since offence occurred	**Offence Seriousness**	**Level of authorisation required**
Less than 60 days	Access permitted for any offence	Self-approval with file number or event number provided as audit trail
60 days to 6 months	Access permitted only for offences punishable by 5 years imprisonment or more	Written approval from Senior Sergeant or above including reference to file number
6 months - 12 months	Access permitted only for offences punishable by 10 years imprisonment or more	Written approval from Inspector or above including reference to file number
Access Requests involving risk to life		
Access to all available records permitted	Reasonable belief a risk to life or safety of any person or a serious threat to public health or public safety exists	Inspector or above Can approve verbally in situations of urgency. Approval must be documented in writing prior to completion of shift.

To provide assurance that retained NPI is only accessed for a legitimate work-related purpose, a CARD event number or NIA file number must be entered in respect of every review completed.

Police use of both Police owned and third party NPI data is subject to oversight and auditing as outlined in this policy.

Police use of ANPR data collected by third parties

VOI data from other Government agencies and third parties may also be utilised in the Police ANPR system e.g., stolen vehicle VOI sub-set. Any such arrangements, whether at District or National level, must be covered by a current letter of agreement (LOA) between Police and the third party that is sharing that data with Police.

The terms of the agreement must give assurance to Police that third party NPI is collected lawfully, make clear the purposes for which that information is being shared, and outline to the third-party Police's obligations for information disclosure under legislation, for instance, in response to Official Information Act Requests. In addition, any network connectivity must meet Police's network security requirements.

All such agreements must be reviewed by Police Legal Services and the Police Chief Privacy advisor before being signed.

Police's existing arrangements to access NPI from third parties has potential to support real-time response plus providing evidential material for investigations and intelligence profiling. Contractual arrangements entered into governing the use of this data must be complied with.

Under current policy, the only VOI data Police can share with third parties, for the purpose of matching to trigger VOI alerts, is the stolen vehicle VOI subset. A stolen vehicle list is published on Police's externally accessible website updated three times a day.

It may be desirable in the future for Police to be able to share a wider range of VOI subsets with third parties (unspecified to those parties) to generate more real time alerts for serious offending and life-threatening situations. The provision of any additional VOI subsets must be approved by an appropriate governance group in Police that has representation of Tier 2 level executive(s).

Arrangements with any approved 3rd party ANPR operators will be defined within appendices attached to this policy specifying details relevant to their capability and the manner in which Police will engage with the party and its system to access NPI. Third party ANPR operators that are currently approved are as follows:

- AUROR
- SaferCities

Any arrangements with additional third-party operators can only be entered into after approval from an appropriate governance group in Police that has representation of Tier 2 level executive(s). If that governance group approves an arrangement with any additional third-party operator the policy will be updated with an appendix specifying details relevant to their capability and the manner in which Police will engage with the party and its system to access NPI.

Approved access and review of third party retained NPI data

NPI captured by third-party providers is retained and stored in accordance with the third-party's own legal and financial parameters. Police will not request any third-party to retain any NPI for longer than 12 months. Any requests to access third-party NPI must be consistent with Police access and approvals process as set out in below table.

Data Access for Offences		
Period elapsed since offence occurred	**Offence Seriousness**	**Level of authorisation required**
Less than 60 days	Access permitted for any offence	Self-approval with file number or event number provided as audit trail
60 days to 6 months	Access permitted only for offences punishable by 5 years imprisonment or more	Written approval from Senior Sergeant or above including reference to file number
6 months - 12 months	Access permitted only for offences punishable by 10 years imprisonment or more	Written approval from Inspector or above including reference to file number
Access Requests involving risk to life		
Access to all available records permitted	Reasonable belief a risk to life or safety of any person or a serious threat to public health or public safety exists	Inspector or above Can approve verbally in situations of urgency. Approval must be documented in writing prior to completion of shift.

Any relevant NPI becomes evidential material in relation to that investigation and can be introduced onto the investigation file as a permanent record.

Police will not enter any arrangement with any third party ANPR provider unless that provider can provide controls on the level of access, approval and auditability set out in this policy and accompanying SOPs.

Approved use of third party ANPR for active detection capability

Stolen VOI subset

Presently there is only one subset of VOI data that is provided to third party ANPR networks and that is the stolen vehicle database which is provided from NIA and refreshed every 15 minutes.

An appropriate governance group that consists of a representation of Tier two Police Executives must approve any additions to VOI subsets being provided to third party ANPR networks before its release. In terms of Police supplying data to non-police networks, care should be taken to ensure all personal information is used and/or disclosed in accordance with the Privacy Act 2020, and that data collected for Police intelligence purposes is not inappropriately released outside Police. Approval of additional VOI subsets being released to third parties requires a privacy impact assessment, consultation with the Office of the Privacy Commissioner, and approval by appropriate governance group before being implemented.

At the present time, Police will be notified in live time of any vehicles that have stolen alerts that are captured on any ANPR camera connected to the third-party network. Districts have their own processes around deployment to any stolen vehicle notifications.

Other Individual VOI

There is existing capability to enable individual vehicles of interest to be uploaded to third party ANPR networks with the intent of obtaining location data of that vehicle at the time it is detected by an ANPR camera. This has the potential to constitute “tracking” as defined in the Search and Surveillance Act.

This can only be done under one of the following three criteria:

Risk to Life or Safety of any person

Where there is insufficient information to suspect an offence, but Police reasonably believe that there is a serious threat to the life or safety of any person or a serious threat to public health or public safety. This includes persons who are considered to be at risk of self-

harm or harm by other individuals. Under these circumstances the active detection capability can be utilised in respect of any specific vehicle(s) suspected to be linked to the incident.

Definition

- ***serious threat*** means a threat that an agency reasonably believes to be a serious threat having regard to all of the following:

a. the likelihood of the threat being realised; and
b. the severity of the consequences if the threat is realised; and
c. the time at which the threat may be realised

- ***reasonably believes*** requires Police to believe the circumstances actually exist. There must be more than a suspicion that something is inherently likely. Further operational examples are provided under the section 'Guidance and examples of acceptable ANPR/NPI use'.

Under a Tracking Warrant

Where Police are operating under the authority of a warrant obtained under the Search and Surveillance Act and that warrant authorises tracking of a particular vehicle or of a person using a particular vehicle.

Under section 48 of the Search & Surveillance Act

Where Police are operating under the urgency or emergency provisions authorised under section 48 of the Search and Surveillance Act 2012 (the Act) which authorise the tracking of a person or vehicle.

The Officer approving the section 48 powers must ensure that a Judges report under section 60 of the Act is completed to a Judge of the appropriate court within 30 days.

Access and approval process

The following table outlines the access and approval process for use of the active detection capability in respect of any third party ANPR networks.

Each individual use of an active detection capability will be subject to audit to ensure compliance with this policy.

Access to active detection capability		
Category	**Criteria that must exist**	**Level of authorisation required**
Where there is a need to prevent or lessen a serious threat to someone's life or a serious threat to public health or public safety, but no offence is suspected	Authorising officer reasonably believes a risk to life or safety of any person or a serious threat to public health or public safety exists	Senior Sergeant or above Can approve verbally in situations of urgency. Approval must be documented in writing prior to completion of shift Name of authorising officer must be included in the text field when entering the vehicle into the third-party network
Under a Tracking Warrant	Authorising Officer confirms that a valid tracking device warrant is in existence for the vehicle	Senior Sergeant or above Name of authorising officer and warrant number must be included in the text field when entering the vehicle into the third-party network
Under section 48 of the Search & Surveillance Act	Detective Inspector or above approves after assessment of whether the criteria outlined in section 48 SSA exists	Detective Inspector or above Name of authorising officer must be included in the text field when entering the vehicle into the third-party network

Governance and Assurance Reporting Model

Primary Governance

The primary oversight and governance of ANPR Policy is the responsibility of Organisational Capability Governance Group (OCGG). The executive sponsor is the Deputy Chief Executive: Insights & Deployment.

The role of the OCGG is to oversee the ANPR programme on a national level and to:

- ensure regular audits are conducted to check compliance with applicable laws, regulations, standards, and policy, including compliance of third parties with Police requirements
- ensure that stored NPI is automatically purged from Police controlled storage facilities at the end of the agreed retention period, unless determined to be of known evidentiary value
- ensure and document that all personnel with authorised access to NPI are trained prior to using the system
- ensure all relevant legislation, policies and procedures are being complied with, and LOA/MOU are kept current
- ensure policy remains applicable and current and to amend accordingly
- appropriately resolve any disputes, ambiguities or policy issues that need clarification.

Other government agency access to ANPR Data

Other government agencies involved in intelligence collection and law enforcement may request Police-owned NPI from Police.

Where possible, access to NPI should be subject to existing agreements that govern information sharing.

In the absence of any existing Policy or agreement, an individual request must be referred to Police Legal Services prior to any NPI being released.

Guidance and examples of acceptable ANPR/NPI use

Acceptable use of ANPR

- A call is received from the mother of a teenager. The teenager has left a suicide note in their bedroom and has taken the family car from the home address and their current whereabouts is unknown. The teenager does not typically use the vehicle they have taken. In this case a person safety alert should be placed on the vehicle, so it becomes part of the Police ANPR data extract. This is also a case where circumstances actually exist to support a reasonable belief that the teenager's life is at risk. Vehicle NPI can also be supplied to any third party ANPR networks Police has access to so that the active detection capability can be enabled so that a notification will be received if the vehicle is detected by a third party ANPR camera connected to a network accessible to Police.
- A call is received by a distressed parent outlining the fact that their partner has breached a parenting order and picked up a 6-year-old child from school in a vehicle for which a registration number was provided. The partner is alleged to be mentally unwell and had made comments to the effect that if they couldn't get full custody then the 6-year-old is better off with 'no one'. A check of NIA confirms the partner has mental health flags for depression and schizophrenia. A recent 2I job is also in the system where a mental health professional has rung Police with concerns that the parent has missed appointments and has not filled a recent prescription. Arguably a tracking device warrant could be sought or S48 powers invoked for a breach of S78 of the Care of Children Act however in this case circumstances actually exist to support a reasonable belief that the 6-year-old's safety is at risk and the safety of the child is the priority. A person safety alert should be placed on the vehicle, so it becomes part of the Police ANPR data extract. and the Vehicle NPI can also be supplied to any third party ANPR networks Police has access to so that the active detection capability can be enabled so that a notification will be received if the vehicle is detected by a third party ANPR camera connected to a network accessible to Police.
- A missing person's report is received from the mother of a 21-year-old student. The mother reports that she has a close relationship with her daughter and usually is in contact with her almost daily either personally or on Facebook or Instagram. The mother last spoke to her daughter 3 days ago on Friday evening and her daughter was about to go to a party. The mother has made contact wither her flatmate who reports that she did not come home on Friday night, and she has not seen or heard from her since. There has been no activity on her social media accounts since Friday evening. The flatmate also has confirmed that she left with her car on the Friday night and her car is not parked in its usual spot on the road outside the flat. Attempts to contact her on her cell phone have gone straight to voicemail. In this case, although the circumstances are suspicious, Police have insufficient information to suspect an offence has occurred. The circumstances however support a reasonable belief that there is a risk to the safety of the student. A person safety alert should be placed on the vehicle, so it becomes part of the Police ANPR data extract. and the Vehicle NPI can also be supplied to any third party ANPR networks Police has access to so that the active detection capability can be enabled so that a notification will be received if the vehicle is detected by a third party ANPR camera connected to a network accessible to Police.
- A person pushes an elderly lady over and steals her handbag. He is seen getting into a vehicle and a witness provides the registration number of that vehicle. The vehicle is not reported stolen. In this case the offence of Robbery is the lead offence. Robbery is punishable by 10 years' imprisonment. The vehicle will have an alert placed on it as "sought "and will form part of the Police ANPR data extract. Due to the offence penalty being 10 years imprisonment, a Senior Sergeant can also approve access to any Police, or Third party retained NPI for location data relevant to that vehicle for the past 6 months.
- Police receive reports of a person being shot in a public place. A suspect is seen getting into a vehicle with a long barrel firearm and the vehicle flees the scene at speed. A witness obtains a motor vehicle registration number. The vehicle will have "sought" and "organisation safety alert" placed on it and will form part of the Police ANPR data extract. Due to the offence penalty being over 10 years imprisonment, an Inspector can approve access to any Police, or Third party retained NPI for location data relevant to that vehicle for the past 12 months. In this case, Police could potentially invoke section 48 of the Act or seek a tracking device warrant so the NPI for that vehicle can be sent to any third party ANPR network that has an active detection capability so that a notification will be received if the vehicle is detected by a third party ANPR camera. If this is done a Judge's report under section 60 of the Act must be completed.
- Covert Human Intelligence Source (CHIS) information is received that is considered reliable that a person is driving a vehicle containing a dealing quantity of a Class A controlled drug. In this case the vehicle can be entered as 'sought' and will form part of the Police ANPR data extract file. There would need to be an appropriately worded alert and expiry date to ensure that any officers deploying to a detection could properly assess whether there were lawful grounds to stop the vehicle. Due to the offence penalty being over 10 years imprisonment, an Inspector can approve access to any Police, or Third party retained NPI for location data relevant to that vehicle for the past 12 months. In this case, Police could potentially invoke section 48 of the Act or seek a tracking device warrant so the NPI for that vehicle can be sent to any third party ANPR network that has an active detection capability so that a notification will be received if the vehicle is detected by a third party ANPR camera. If this is done a Judges report under section 60 of the Act must be completed
- A surveillance device warrant seeking authority to use a tracking device for an offence punishable by imprisonment is granted. Under that warrant any vehicle for which tracking is authorised could be entered as 'sought' and it will form part of the Police ANPR data extract file. Individual vehicles may also be entered into an approved third-party provider so that a notification will be received if the vehicle is detected by a third party ANPR camera connected to the network. A Senior Sergeant can also approve access to any Police, or Third party retained NPI data for location data relevant to that vehicle for the past 6 months.

APPENDIX A - NPI From Police owned ANPR Cameras

Current state

Police currently utilises mobile ANPR cameras which are placed into Police owned vehicles. Each district has this capability. A smaller number of Districts have also invested in static ANPR cameras.

NPI data from Police owned ANPR cameras is currently underutilised and is not generally available for the law enforcement purposes outlined in this policy. There is no centralised storage or review solution.

Current mobile ANPR camera in vehicle ANPR upload procedure

The data obtained from ANPR deployments consists of:

- a list of registrations captured by the ANPR camera, including date, time and location;
- an image of a registration plate; and
- an image of part or all of the vehicle (depending on how the camera is set up).

At the end of every shift, the ANPR operator must where applicable:

- upload data from the ANPR system to an encrypted flash drive; and
- on return to their Police station, transfer the data to the BOSS system.
- The data may be manually processed and deleted, or the BOSS system will automatically delete the data after 48 hours.

All ANPR data retained for processing must only be stored in the J: Drive, ANPROVI folder, Endshift folder, and into your respective districts folder. If records are in excess of 48 hours old and the software is activated, the system will automatically delete the data.

If you have access to BOSS Server, download the Iron-Key directly onto the standalone BOSS laptop by completing a synchronisation. The data will be of no use if it is processed after 48 hours from the time the read or hit was obtained, as BOSS automatically deletes the information after this period.

Future state

Police proposes to identify a suitable retention and storage solution for Police owned and generated NPI. This would allow storage of NPI for up to 12 months and access to that data in accordance with the access and approvals section of the Policy and SOPs.

APPENDIX B - NPI provided by AUROR

Current state

AUROR is a Retail Crime Intelligence Platform that has been developed to help retailers report, solve, and prevent crime. It enables this through a user-friendly interface which encourages more crime to be reported in a structured way. Retailers and other organisations can choose to share information with NZ Police through the Platform. This includes providing Police with the ability to make limited access requests to NPI data generated from ANPR cameras situated on their premises.

AUROR retains NPI in accordance with each NPI provider's own privacy policies. Any NPI retained by AUROR is deleted after **60 days**.

Individual Police users can obtain a login to the AUROR network and can access the following functions relevant to NPI;

Find a vehicle

Reviews of vehicles for historical detections in the past 60 days may be carried out in accordance with the access and approvals process in the ANPR policy and SOPs.

Track a vehicle (Active detection capability)

A registration number of an individual vehicle can be entered into the AUROR ANPR network. If that vehicle is detected by a camera on the network, the requestor will be notified in real time of that vehicle's current location.

This capability can only be used in accordance with the access and approval process for active detection capability in the APNR policy and SOPs.

Audit and oversight

Each time an individual user reviews a vehicle, they must enter a relevant police file number before they can view the NPI. All of the information related to each review is stored in logs by AUROR for a period of not less than three years.

When a user tracks a vehicle, they are required to enter their supervisor's ID and upload a warrant document (where applicable). A notification of this request is automatically sent to the supervisor.

AUROR also provides Police the following data to audit:

- User Access Data
- All reviews completed by an individual user for a period of three years.
- All "track" a vehicle requests completed by an individual user for a period of three years.

APPENDIX C - NPI provided by SaferCities

Current state

vGRID ANPR is a platform that enables Police to connect to ANPR sources nationally (Police owned and third party). vGRID ANPR creates opportunities for Police to access ANPR networks connected to the SaferCities network to obtain historical and real time NPI data. Third parties can choose to share information with NZ Police through the Platform. This includes providing Police with the ability to make limited access requests to NPI data generated from third party ANPR cameras.

SaferCities retains NPI in accordance with each NPI provider's own privacy policies. NPI data is currently retained for a period of **6 months**. Access for reviews is permitted in accordance with the access and approval process in the ANPR Policy and SOPs. Individual Police users can obtain a login to the SaferCities platform and can access the following functions relevant to NPI:

ANPR detection

Reviews of vehicles for historical detections in the past 6 months may be carried out in accordance with the access and approvals process in the ANPR policy and SOPs.

Plates of interest (Active detection capability)

The Plates of Interest function allows a user to receive an alert via the vGRID SaferCity App (desktop or mobile) or email alert in real time when a vehicle registration number they have sought is detected in the camera network. This capability is deployed with the NIA Stolen Vehicles / Plates sought list publicly available. Plates of Interest not on this sought list can only be used in accordance with the access and approval process for active detection capability in the ANPR policy and SOPs.

Audit and oversight

Police use of NPI is governed by a master service agreement with SaferCities and this policy.

Audit and logging

The event information for all use of license plate detections including Plates of Interest and Detection reviews is held in the event logs. SaferCities retains this centrally held log of all relevant user access and event activity indefinitely. These activity logs are available to Police on request.

SaferCities is able to provide Police the following data to audit:

- User Access Data
- All reviews completed by an individual user
- All "plates of interest" vehicle requests completed by an individual user

SaferCities is currently considering the appropriate length of time to retain these event records having regard to information management best practice and the Chief Archivist Guidelines. SaferCities may eventually determine it not necessary to retain user logs permanently. Their current expectation is that logs shall be kept for a period not less than 3 years. SaferCities will notify Police upon any decision to vary their practice to anything less than indefinite retention.

APPENDIX D: Standard Operating Procedures

Requests for Information of Number Plate Information (NPI) from ANPR technology

Police requests of NPI data collected by third parties

1. Introduction

These Standard Operating Procedures (SOPs) set out instructions for Police engagement with a third-party provider of Automated Number Plate Recognition (ANPR) capability.

NPI data includes a still image of a vehicle number plate, an optical interpretation of the number plate shown in the image, a geographic location, and date/time stamp of the image capture. Available data may also include video footage of a vehicle captured at the same time as the ANPR data.

This combination of data acquired from a third-party provider (e.g., retailers, government organisations) may be classified as personal information (Privacy Act 2020). Police may acquire the NPI data through a general Request for Information (RFI), or by executing a production order, search warrant or tracking warrant.

2. Purpose

These SOPs set out the way Police are required to correctly engage with third-party providers. Guidelines include the way that RFIs are to be completed and Search and Surveillance Act actions are to be authorised and entered into a platform (e.g. Auror and SaferCities) facilitating the request.

3. Duties and responsibilities

The management of the information stored within a platform that facilitates the transfer of the information from a third-party provider is the responsibility of that third-party collecting and providing that data. This can be enabled through platforms like Auror and SaferCities who provide a service to third-parties by storing and processing it for them under the third-parties direction. This means that a request for NPI from these platforms is an activity between Police and the retailer/government organisation; not Police and Auror/SaferCities.

Auror and SaferCities act only to facilitate the request and/or transfer of NPI between a third-party i.e., retailers/government organisations, and Police. The third-party remain responsible for the use and disclosure of the information within the platform.

3.1 Third-party providers

Where an RFI is made for NPI, or a warrant is served via the platform, the third-party providers are responsible for ensuring that the automated process set up within the platform they use facilitates a response that is lawful and necessary. Where a production order or a warrant is executed via a platform, details entered by Police will authorise a mandatory response.

When an RFI is made by Police, the third-party providers are required to comply with Information Privacy Principle 11(1)(e)(i) of the Privacy Act 2020. This legislative provision requires the third-party provider to believe on reasonable grounds that the information requested by Police meets an exception in IPP 11 to avoid a prejudice to the maintenance of the law, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences.

The third-party provider must be satisfied that it is appropriate to release the requested information to Police. In usual business circumstances such as a face-to-face interaction, appropriate questioning by the third-party provider would be enabled. Automated platforms do not easily facilitate request scrutiny by the third-party provider. A platform's request mechanism therefore requires adequate detail to satisfy the requirement that Police's requests are reasonable and necessary.

3.2 Police - RFI Requests

- To satisfy the law
- To meet obligations to provide sufficient information to enable the third-party providers to disclose NPI data staff must:

i. Enter a valid Police record number (File number or Card number) into the request; and
ii. Select the type of Police activity from the drop-down menu in the request (drugs; homicide; sexual offence; violent crime; volume crime; other; prevent or lessen a serious threat -IPP 11(1)(f)*; and
iii. In the free text box explain why the NPI data is needed and how it is connected to the Police activity.

*Note: Information Privacy Principle 11(1)(f) Privacy Act 2020 'that the disclosure of the information is necessary to prevent or lessen a serious threat to public health or public safety; or the life or health of the individual concerned or another individual'

Examples of an explanation when requesting NPI from a third party
The car was seen leaving the scene of a burglary during the period when the offence was committed in circumstances that suggest the occupants were involved in the crime.
Witnesses identified the car as the vehicle involved in a hit and run motor accident and we believe it is the offending vehicle because of other evidence gathered at the scene.
Police are investigating a serious drug related crime and this vehicle is closely associated with key persons of interest and we believe the car and occupants are involved in the organised enterprise.

3.3 Police - Search and Surveillance Act or urgency

- To satisfy the law
- To meet obligations to provide sufficient information to enable a provider to disclose NPI data by tracking a vehicle over a specified time, staff must:

i. Enter a valid warrant number where a tracking warrant or other judicial process has been issued; or
ii. Enter a valid Police record number where the search is undertaken pursuant to section 48 of the Search and Surveillance Act, and clear reasons for the acquisition of NPI by tracking the vehicle must be included in the free text box; or
iii. Enter a valid Police record number where the search is required to prevent or lessen a serious threat to life, public safety or health and no offence is suspected, and clear reasons for the acquisition of NPI by tracking the vehicle must be included in the free text box; and
iv. In all cases the authorising officer's email must be included in the appropriate field and their name included in the free text box.

3.4 Police - Use of the Platform

To meet Police assurance requirements

Use of the Platform is governed by the same rules as accessing any other Police system. You should only access on approved police devices for official purposes while actively on duty in accordance with the law and in compliance with Police policies.

To enable Police to provide full assurance over use of the Platform staff must :

i. Enter a valid Police enterprise email into the request;
ii. Enter the valid Police enterprise email of an appropriate manager who is either involved in the investigation or the requester's manager, and for requests for information over 60 days, has the requisite seniority to approve the request;
iii. If the access to NPI data is sanctioned by a warrant, enter the correct warrant number into the request and in the free text box, a brief reason for the existence of the warrant;
iv. Where the search is pursuant to a without warrant power (s 48 of Search & Surveillance Act) explain in the free text box a brief reason for the power being invoked, the name of the approving Detective Inspector, and add a file number to the request; and
v. Fill in the free text box with an adequate reason why the NPI is necessary for Police purposes.

Manual checking of NPI data acquired from the Platform

Upon receipt of the NPI data package staff must ensure that the system has interpreted the image correctly by manually checking the image of the vehicles number plate against the information provided in the package to ensure that there is a reliable match. Where there is doubt about the match the NPI data should not be used unless there are other corroborating factors that render the NPI

relevant to the investigation.

4. Governance and Assurance

Governance responsibility

Maintaining good assurance practices regarding Police engagement with the platform holders is crucial to good governance and oversight. To achieve appropriate assurance the governance group shall require regular reporting that includes the volume of interaction with a platform, regular audit results, and approving transparency reporting.

Platforms Auror and SaferCities maintain audit logs that are available to Police. The logs capture user access data, reviews completed by an individual user for a period agreed to by the platform provider (not less than three years); and all "track" a vehicle requests completed by a user for a period agreed to by the platform provider (not less than three years).

Auror and SaferCities are also able to supply Police with a list of high-volume users of their platform.

4.1 Interaction with the Platform

Transparency is key to maintaining public trust and confidence. Reporting that demonstrates the overall general usage of the site provides transparency and demonstrates Police's commitment to the proportionate use of technology. The Governance Group shall approve yearly (or 6 monthly) reporting that includes:

- The number of times staff have used the platform to request NPI data
- A summary of the reasons why NPI data was requested using the platforms provided selection criteria in "Select the types of crime that apply" - drugs; homicide; sexual offence; violent crime; volume crime; other.
- Commentary about the success of NPI data in solving crime or reducing serious threat to individuals
- Commentary about the appropriateness of the activity of high-volume users of automated ANPR platforms.

4.2 Audit

Audit of staff access to these platforms is also important in demonstrating Police's appropriate use of these technologies. It also provides a deterrent to staff who may use the system unlawfully or inappropriately. Depending on the volume of usage, an audit might be confined to a random and representative review of requests. Audits shall be completed every three (3) months and record:

- The level of compliance with the requirements to include a valid Police record or warrant number
- The adequacy of the reasons why the NPI data is needed and how it is connected to the stated Police requirement
- The level of compliance with appropriate manager authority for 'track' a vehicle request
- The legitimacy of Police record numbers and warrant numbers

Results of an audit must be assessed, and discrepancies appropriately responded to.

Examples of inappropriate use and potential remedial actions
Use of ANPR generated information outside this policy may be considered unauthorised use and subject to an employment investigation which could lead to disciplinary action.
Where a system fault or process fault is detected in audit results the governance group must direct and authorise an appropriate change to the system.
Where an individual user is not using the system or process correctly a discussion is to be held with the staff member and their supervisor to identify and explain the error in use, and seek a commitment to change behaviour.

4.3 Transparency Reporting

Communicating publicly about how Police is using personal information and technology enhances public trust and confidence. The Governance Group shall approve transparency reporting to be included in an appropriate place on Police's public website. The reporting should be at least annual and include -

- The number of requests, warrants and other statutory processes that have been used to access NPI data;
- A summary of the reasons why NPI data was obtained using the platforms provided selection criteria in "Select the types of

crime that apply" - drugs; homicide; sexual offence; violent crime; volume crime; and other;
- A high-level overview of the successful results of acquiring and using NPI data from platforms Police has access to; and
- A high-level view of the level of compliance by Police staff with the ANPR policy including these SOPs.

5. Review

The SOP guidelines outlined above represent a living document. The SOP is to be evaluated and updated annually or following any incident. A review must assess whether there is a need for changes to the way Police engages with ANPR platforms and the changes shall be reflected in a revised set of SOPs and policy as necessary.

ANPR Vehicle Operating Procedures

Introduction

The purpose of the ANPR Vehicle Operating Procedures is to ensure staff maximize enforcement, staff safety and public safety opportunities for the use of ANPR enabled vehicles and use these tools in accordance with the ANPR policy and legislation.

Key, critical points for staff to note:

- Only approved ANPR deployment methods and equipment are to be used.
- ANPR equipment must only be operated by Police who have completed formal training.
- The ANPR system is only as effective as the data quality relating to the alerts - staff should correct and update any discrepancies.

Overview

ANPR is a technology used to automatically identify vehicles of interest (VOI), as flagged in the National Intelligence Application (NIA), Motor Vehicle Register (MVR), and Driver Licence Register (DLR), from their number plates.

The ANPR system uses optical character recognition (OCR) to scan vehicle number plates and check them against VOI alerts. In simple terms it assists officers by negating the need to refer to lists of VOIs by informing them when such a vehicle is detected by the system. When a VOI is recognised, the system alerts the operator who can take appropriate action.

This document sets out:

- an overview of ANPR equipment
- approved methods of deployment; and
- the procedures to be followed during the deployment of ANPR

Note: This chapter applies to Police constables and authorised officers, hereafter referred to collectively as 'Police'.

ANPR equipment

Components

ANPR systems are made up of these components:

- a camera
- a computer; and
- a monitor

Software

ANPR systems use software which has limited support from the Police Information and Communication Technology (ICT) helpdesk. Instructions on software operation and support contacts are included in the training given to ANPR operators.

Servicing

Instructions on software and hardware servicing are included in the ANPR operator manual.

ANPR vehicles

ANPR equipment must only be operated in purpose built ANPR vehicles in accordance with this ANPR Vehicle Operating Procedures. If it is operationally necessary to alter the vehicle or operate ANPR in any other manner, pre-approval must be gained from the Director:

Road Policing prior to any change being made or organised - refer to the Police vehicle management chapter.

Training

ANPR equipment must only be operated by Police who have completed formal training from Road Policing Support staff or have received formal training from an employee in their district who has used ANPR and is competent in its use.
To ensure national consistency and quality of content and delivery, all training must be approved by the Director: Road Policing; and comply with the quality assurance standards set by the Police Training Service Centre (TSC).

Roles and responsibilities

This table sets out the roles and responsibilities associated with ANPR equipment.

Role	Responsibilities
Director: Road Policing	- Must approve the ANPR training session content. - May approve (in writing) requests to operate ANPR in non-standard deployments or outside of these guidelines.
District Commanders	- Must ensure Police are trained to operate ANPR equipment prior to authorizing operational deployment.
Officer in charge of ANPR operations	- Must ensure all operational deployments of ANPR: - have a trained ANPR operator. - are used in a manner that enhances road safety and enforcement opportunities; and - maintain business as usual.
ANPR operator	- Must have completed an ANPR training session. - Must have read and understood the ANPR operator manual.
ANPR vehicle	- Must not be altered except by prior written approval from the Director: Road Policing. - Vans must be used as a category D vehicle and not be used to transport or hold prisoners. - Marked patrol vehicles fitted with ANPR are still a category A vehicle.
Support vehicles	- These must be category A or B patrol vehicles. They should be operated by gold classified drivers.
ANPR Intercept Team	- Must be aware of their powers when acting on a VOI alert as identified by ANPR.

ANPR operations - approved deployment models

Pre-deployment procedures

- All deployment types

Follow these steps for all deployment types.

Step	Action
1	Ensure appropriate Police resources are available to conduct the type of approved deployment: ANPR_operations_-_approved_deployment_models.doc
2	Conduct a briefing on Police roles, responsibilities, and operational focus, i.e. high-risk drivers and alerts.
3	Ensure the ANPR equipment is ready to operate. The ANPR van also requires the batteries to be checked.
4	Ensure the ANPR operator obtains an up to date begin-shift folder containing the latest alerts.
5	Ensure the ANPR camera is set-up correctly: · **For static deployments**, set up the ANPR vehicle ensuring it is legally and safely parked. The vehicle's position must not disrupt the normal flow of traffic. · **For mobile deployments** where cars may be parked, the vehicle's camera angles may be adjusted prior to arriving at the deployment location. **Note**: Sometimes ANPR is best suited in the middle of the road, scanning both lanes (oncoming / away).
6	Inform the Communication Centre (Comms) of the nature and location of the ANPR deployment.

- Limited scale deployments

Follow these steps for limited scale deployments.

Step	Action
1	For mobile deployments, ensure the ANPR vehicle driver does not monitor the ANPR equipment while driving. If you are one-up, pull over before checking the VOI alert.

- Checkpoints

Follow these steps for checkpoints.

Step	Action
1	Prepare a deployment plan including a site plan.
2	Ensure adequate signage and cones are available.
3	The ANPR operator must ensure the intercept vehicles and checkpoint Police are in position and ready prior to commencing a deployment.

- Mobile deployments

Follow these steps for mobile deployments.

Step	Action
1	For mobile deployments, ensure the ANPR vehicle driver does not monitor the ANPR equipment while driving.

- Non-standard deployments

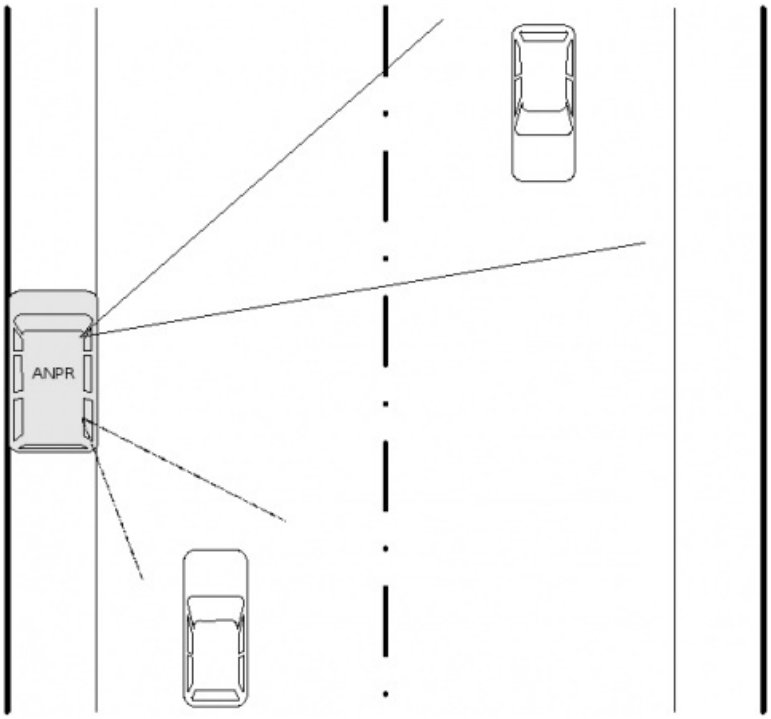
For non-standard deployments, such as Impairment Prevention Teams, comply with their standard operating procedures.

ANPR deployment site plan examples

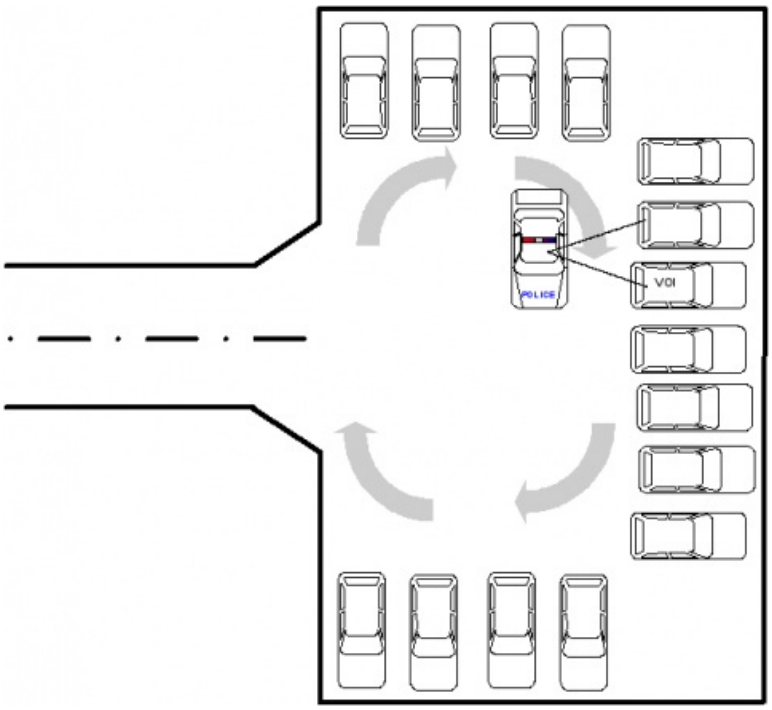
Generic examples

These are generic examples to assist the officer in charge of an ANPR operation with the preparation of site plans. For Impairment Prevention Team checkpoints refer to the 'Alcohol and drug impaired driving' chapter.

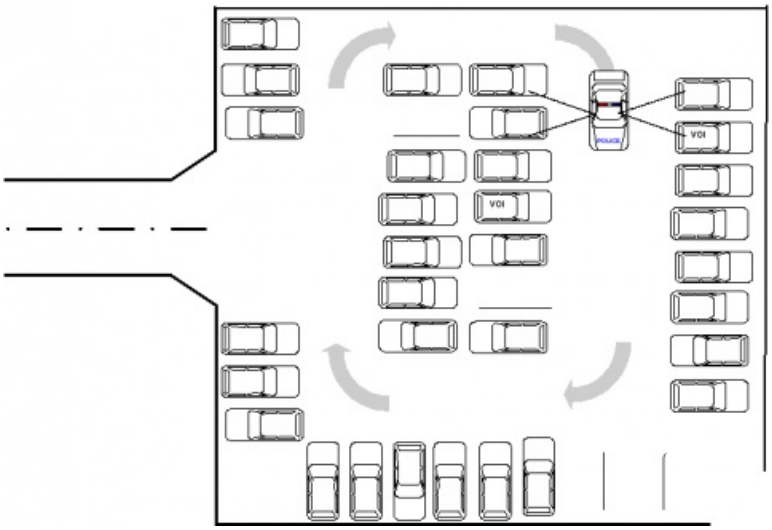
Parked deployment



Car park deployment

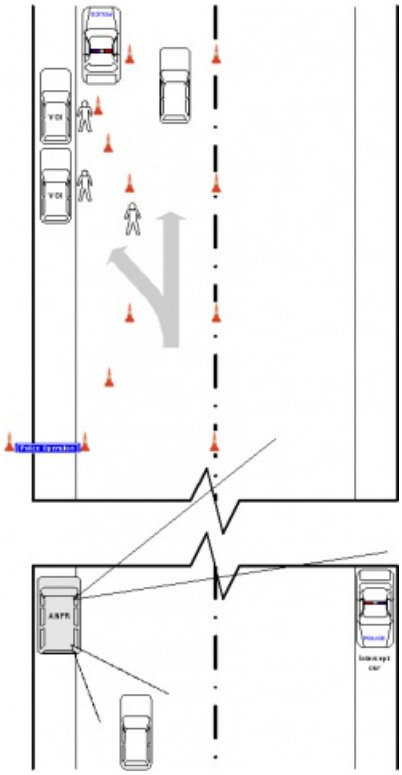


- Left parking mode -



- Dual parking mode -

ANPR checkpoint



- Single/dual traffic direction mode -

Note: The ANPR van/marked patrol vehicle can be set to read traffic in both directions where the checkpoint operates in both traffic directions.

Selecting a location

Points to consider

When selecting a location for all deployment types consider the Police Manual chapter 'Perimeter control'. For ANPR checkpoints also consider this table.

Consider	Rationale
The deployment model (see below)	Not all deployment models are suitable for all locations.
Traffic volumes	To maximise the potential of ANPR, higher volumes of traffic are recommended. Only a small percentage of vehicles have VOI alerts.
Intercept risks	Consider deployment sites which allow easy migration of the ANPR or intercept vehicle into traffic flow and limit an offender's escape routes. Areas with side roads or additional potential for offenders to do u-turns increase intercept risks.
Officer/public safety	Avoid areas where drivers have little reaction time prior to arriving at a checkpoint, or there is a risk of nose-to-tail crashes if traffic begins to queue. Avoid areas with poor overhead lights at night.
Hazard creation	The ANPR vehicle should be legally parked and in a manner that ensures the operator's and public safety.
Service disruption	Avoid checkpoints that disrupt the flow of emergency service vehicles, e.g. near Police or fire stations. When operating with a Impairment Prevention Team ensure the ANPR intercept team operates behind the Impairment Prevention Team.
Sufficient room for the intercept team and vehicles	The intercept team needs enough space to safely process VOIs, including room to tow impounded vehicles.
Local knowledge	Police will know areas where successful operations have been conducted in the past.

-

ANPR_operations_-_approved_deployment_models.doc 59 KB

ANPR checkpoint procedure

Radio procedures

Where possible, only use Mobility devices for communications to limit radio traffic. Follow these steps (not necessarily in the order shown here).

Step	Action
1	Ensure Comms are aware of the nature and location of the ANPR deployment and at least one member of the intercept team monitors the main radio channel.
2	Ensure support vehicle radios remain on the main radio channel so that communication is on the main channel if an offender fails to stop when signalled to do so. For further information refer to the 'Radio and Emergency Communication Centre Protocols' chapter.
3	Use a closed simplex channel for communication between the ANPR operator and intercept team. This channel should be kept free to allow the ANPR operators to broadcast the VOI alert type and description.

Note: The intercept team should only communicate to acknowledge the VOI alert or when they are all busy and do not require further alerts to be broadcast.

ANPR equipment setup

Refer to the ANPR Operator Manual.

ANPR checkpoint setup

Follow the site plan and for positions of the ANPR vehicle, support vehicles, signage and cones.

VOI alerts - ANPR operators

ANPR operators must follow the procedure in figure 1 below when a VOI is detected.

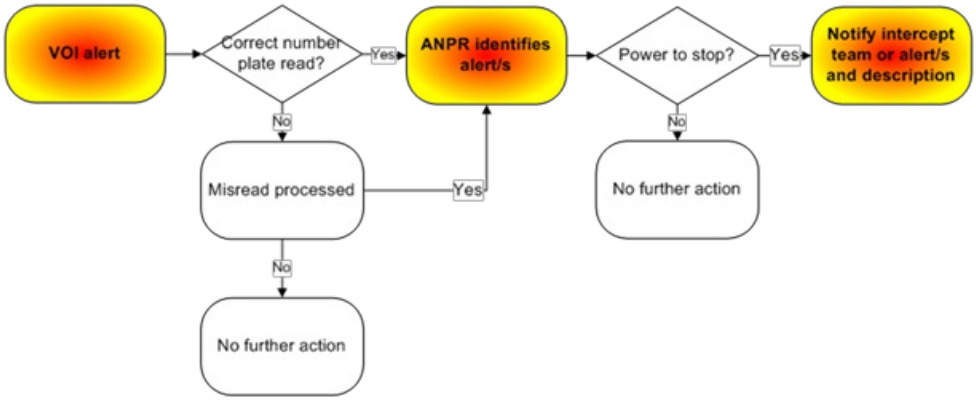


Figure 1: ANPR operators' decision chart

Plate misreads

The ANPR OCR software may occasionally misread similar shaped characters such as a '1' as an 'I', or an 'O' as a 'Q'. The ANPR operator must compare the photograph of the captured plate with the OCR definition to determine if the plate has been read correctly.

Multiple VOI alerts

The ANPR software does not prioritise VOI alerts in order of seriousness, where a detected vehicle has multiple VOI entries. Prior to informing an intercept team of VOI activity, all VOI alerts for the detected vehicle must be assessed and prioritised. The ANPR operator must ensure that the VOI information passed to the intercept team accurately reflects all information held on the detected vehicle. This enables the intercept team to assess the threat level and plan accordingly in accordance with 'TENR'.

VOI alert - intercept team

Once notified of the alert type and vehicle description, the intercept team can prepare to stop the vehicle. Depending on the alert type consider:

- the statutory obligations pursuant to the power to stop under the Search & Surveillance Act 2012;
- the risk the driver may fail to stop; and
- the risk the driver or passengers may flee on foot.

For more information on stopping vehicles refer to: 'Traffic patrol techniques'.

If a vehicle fails to stop, follow the 'Fleeing driver policy' and 'Urgent duty driving' policies. Intercept staff should be aware that a VOI, failing to stop on request, does not automatically provide sufficient grounds to pursue the fleeing vehicle.

Approaching the driver

For information on approaching the driver of a vehicle refer to: 'Traffic patrol techniques'.

Acting on the alert

Remember that some VOIs may no longer be of interest to Police but are yet to be expired. This must be considered when dealing with the driver.

For information on actions to be taken when acting on the alert refer to the appropriate Police Manual chapter. The main chapters are listed below:

- 'Alcohol and drug impaired driving'

- 'Arrest and detention'
- 'Driver licensing'
- 'Impounding vehicles'
- 'Issuing non-operation orders'
- 'Motor vehicle offences'
- 'Motor vehicle registration and licensing'
- 'Motor vehicle noise enforcement'
- 'Offence notices'.

Following the stop

If it is necessary to do so, update or expire theNIA alert to reflect the current status of the vehicle or notify the agency responsible for the source data. Ensure that intelligence notings are submitted in a timely manner.