Automated Number Plate Recognition (ANPR) Policy (Surrey and Sussex) (1002/2024)

Abstract

This policy describes the Surrey Police and Sussex Police approach to gathering intelligence and identifying vehicles of interest, such as stolen vehicles, or those vehicles suspected of being involved in the commission of a crime or terrorist activity. When a suspicious vehicle is recognised, it allows targeted interception and enquiries.

Policy

1. Introduction

1.1 Automatic Number Plate Recognition (ANPR) is used to help detect, deter, and disrupt criminality at a local, force, regional and national level, including terrorism offences, major crime, serious and organised crime, modern day slavery offences, vulnerable and missing persons, casualty reduction and anti-social use of motor vehicles. The effective and efficient use of ANPR technology will allow Surrey Police and Sussex Police (hereafter referred to as the Forces) to carry out targeted interception as well as lines of enquiry and evidence gathering in the investigation of crime.

1.2 This document will ensure a consistency that meets the National ANPR Standards for Policing and Law Enforcement (NASPLE) in the use and development of ANPR systems and complies with the National Police Chief Council (NPCC) Approved Professional Practice (APP) in disrupting criminality.

2. Scope

2.1 The procedures associated with this policy.

• Cover the use and protection of ANPR infrastructure, access levels and audit.

• Establish clear procedures for police officers and police staff involved in the ANPR process as well as identifying responsibilities specifically related to posts within each Force.

• Cover evidential use and disclosure of data.

3. Policy Statement

3.1 The Forces are committed to supporting the aims of the national NPCC strategy to ‘target criminals through their use of roads’. The Forces continue to maximise the opportunities to bring offenders to justice as well as utilising and exploiting the full potential of ANPR in the search for high risk vulnerable and/or missing persons and safeguarding the public, whilst ensuring that the provision and use of the ANPR infrastructure is carried out in full compliance with relevant legislation.

Procedure

1. Introduction

1.1 National ANPR Standards for Policing and Law Enforcement (NASPLE) describe the standards that are to be met for the development and use of ANPR systems. Follow the link for the current NASPLE.

2. Strategic Leadership

2.1 The Chief Officer lead for ANPR matters is the Assistant Chief Constable (ACC) for Operations Command and the Strategic Lead is the Operations Command Roads Policing Unit (RPU) Superintendent.

3. Infrastructure Development and Deployment of Number Plate Reading Devices (NRD)

3.1 Infrastructure Development will be in accordance with NASPLE Part 2 Para 8.

3.2 All proposals for new infrastructure will be submitted to the ANPR Manager who is responsible for confirming that the proposals are appropriate, ethical, and proportionate, taking account of strategic assessment and Data Protection Impact Assessment (DPIA), in balancing protection of the public with the rights and legitimate expectations of individual privacy. Confirmation is required before any development is progressed.

3.3 The ANPR Manager will ensure that arrangements are in place for review of the locations of all NRD that submit data to the ANPR system at least annually to ensure that the deployment remains appropriate, proportionate and necessary.

3.4 Vehicle mounted ANPR systems will be deployed in accordance with NASPLE Part 2 Para 8.7.2 ‘A moveable ANPR system is one that has been built for the primary purpose of ‘capturing’ and ‘reading’ vehicle registration marks (VRMs) and is located within a police vehicle’.

3.5 A re-deployable ANPR camera can be used in a fixed position on a temporary basis. Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM. Re-deployable ANPR cameras can be bid for via the Daily Management Meeting (DMM) structure. The ANPR Data Officer must be consulted prior to a bid submission to prevent duplication of camera locations.

4. Vehicle Markers

4.1 The Police National Computer (PNC) is the primary database to support operational response. Within the PNC application the ACTion (ACT) report is the primary database for ANPR. PNC is used for the circulation of any vehicles of interest (VOI) which meet the required criteria.

4.2 ACT reports are designated as High, Medium, and Low priority. During periods of increased demand on resources, with the authority of Inspector or equivalent staff grade within the respective control room reports of matches against other forces VOI hotlists may be filtered such that they are not monitored. High and medium priority ACT reports

must be continuously monitored. Low ACT markers can be triaged, and staff are empowered to quickly dismiss those that are not a threat to the organisation.

This process is determined by each Force's local guidance around the deployment of staff to ANPR activations by the respective control room. For detailed information on the deployment process, Lost or stolen vehicles, PNC ACTion markers for theft of number plates and suspected cloned plates see Deployment for Activation Guidance Document.

4.3 VOI, locally known as 'hotlists' may be used to circulate vehicles for intelligence monitoring purposes or in circumstances that do not meet the standards for inclusion on the PNC as an ACT report for operational response. Local hotlists will be uploaded to the National ANPR Service (NAS) via the Forces ANPR management server, other forces or law enforcement agencies can monitor on the NAS or download them to their respective BOF.

4.4 The designated member of staff who is authorised (by the ANPR Manager) to create a hotlist will ensure that the information within it is accurate, of current relevance and in the format prescribed within NASPLE.

4.5 The ANPR Data Officer or nominated ANPR operative will monitor the creation, use and maintenance of hotlists for operational response purposes. Reporting concerns will be directed to the ANPR Manager.

4.6 The Central Authorities Bureau (CAB) in Sussex and RIPCOM in Surrey will ensure that arrangements are in place, to monitor the creation, use and maintenance of a hotlist for intelligence monitoring purposes, where a Regulation of Investigatory Powers Act (RIPA) directed surveillance authority is required.

5. Cross Border Working

5.1 Where a high priority ACT report enters or leaves the Forces borders, it is the responsibility of the designated Inspector within the respective control room to inform neighbouring forces and provide a briefing using the National Decision Model (NDM) in relation to the vehicle and the circumstances.

6. Performance Evaluation

6.1 The ANPR Manager is responsible for monitoring the performance of all components of the ANPR Infrastructure to ensure compliance with NASPLE.

6.2 The performance of NRD will be assessed on installation to ensure compliance with NASPLE and thereafter at least annually to ensure they are running efficiently.

7. ANPR Back Office Data Access

7.1 The ANPR Manager is accountable for the authorisation of police officers / police staff that may access ANPR back-office data. They will ensure that a record of authorised staff is maintained, and that authorisation is reviewed, amended, or cancelled on change of role as appropriate. Officers or staff leaving the Forces should have their accounts deleted within 48 hours.

7.2 Staff may only be granted access to ANPR data to the extent that is necessary for their role. To gain access to the NAS staff must complete the College of Policing learning packages.

• National ANPR Service Foundation Course (Basic Access)

• NAS ANPR Dispatcher Course

• NAS Convoy Search (Advanced Access)

• NAS Cross Search (Advanced Access)

Each course will require a pass / fail test at the end, once completed download the ‘completion’ certificate and email to the ANPR Team will build an account and email the log in and password to the new account holder.

The NAS link can be found on the front page of the intranet under ‘manage my key apps and links’. Save the National ANPR Service to the favourites folder.

7.3 Staff accessing ANPR data must ensure that the access is appropriate in each case taking account of NASPLE, and that it has been properly authorised when required. Staff requiring searches beyond 90 days must have the authority of an inspector or police staff equivalent and contact the ANPR Team for completion.

7.4 Staff authorising access to ANPR data must ensure that access is proportionate and in the interest of justice in each case taking account of the UK General Data Protection Regulations (UK GDPR), Data Protection Act 2018, NASPLE data access provisions. See NASPLE Part 3, Appendices B and C.

Individuals that do not have the necessary training and access must contact their local intelligence unit, regional or 24/7 intelligence teams who can perform searches on their behalf in the first instance.

8. Evidential Use and Disclosure of Data

8.1 The Surveillance Camera Codes of Practice recommends that ANPR data is used to support a prosecution. The ANPR Manager, or other designated person, will be consulted before preparation of disclosure schedules under the Criminal Procedure and Investigations Act 1996 (CPIA) provisions and before any data is used as evidence in any proceedings. ANPR evidence packs will only be supplied by trained staff in the ANPR Team post charge where the use of the data is necessary or at the written request of the Crown Prosecution Service (CPS).

If the team are not available to complete this immediately the use of the data can be supplied to the CPS in an intelligence format as this data is more informative than an evidence pack around locations. It must be logged as sensitive information.

The evidence pack will be supplied at the earliest opportunity by the ANPR Team.

8.2 The disclosure of ANPR methodology, tactics and camera locations will be avoided whenever possible, subject to CPS guidance in order to ensure the continued value of ANPR as an operational and investigative capability. The following paragraphs provide a

framework to support this objective. Concerns regarding disclosure or evidential use will be referred to the Strategic Lead for consideration.

8.3 Statements of evidence may only be provided by staff designated by the strategic lead. It is accepted that the CPS now expect the evidential element to ANPR within files to assist them with their charging decisions. When this occurs, advice to officers includes where the ANPR evidence is a key evidential part of the investigation then this will be accepted as a CPS request to see the evidence.

8.4 During an investigation, ANPR images, investigation methodology, tactics, and maps indicating the locations of ANPR cameras will NOT be disclosed to suspects or their legal advisors without the approval of the ANPR Manager or another designated person and CPS. All ANPR material must be marked as 'Official-Sensitive' unless agreed for court disclosure. The exact location of any camera must not be identified on a map, the advice is to generate a box system around an area the camera is located.

8.5 The ANPR Manager or other designated person will provide advice and guidance in conjunction with the Information Commissioner's Office (ICO) and the Home Office on the information that may be revealed in each case.

8.6 Statements of evidence will only be prepared after proceedings have been initiated or following specific request of the CPS. All requests will be referred to the ANPR Manager or other designated person for authorisation to provide evidential material. They will liaise with the CPS staff making the request and refer to the strategic lead for ANPR for consideration in cases of concern.

8.7 ANPR material not used in evidence will be included on the Schedule of Sensitive Material.

9. Misconduct and Internal Investigations

9.1 In order to properly protect our information and maintain public trust and confidence in line with the expected standards of professional behaviour and the Code of Ethics. The Forces will consider any apparent breaches against the Data Protection Act, Computer Misuse Acts, or other offences. All breaches may be investigated as a criminal offence which may lead to prosecution or disciplinary proceedings.

9.2 ANPR data will be available for research and evidence produced in cases where officers and staff are suspected of having breached the standards of professional behaviour. This requires the written authority of a Superintendent or above as per NASPLE.

10. Records of Data Access and Audit

10.1 The ANPR Manager ensures that provisions to provide a record of access to ANPR data by their staff, including the reason for that access and details of any authorisation of that access where required.

10.2 The ANPR Manager will ensure that provisions for regular audit of access to ANPR data are in place, with a record of all audit activity that has been undertaken in line with the national auditor's guidance.

10.3 Where data has been accessed for which the data controller is from another Law Enforcement Agency (LEA), the data will be provided to that data controller on request.

10.4 Details of audits undertaken will be made available to the ICO, the Surveillance Camera Commissioner on request.

10.5 Data retention periods for all data are contained in the relevant NASPLE Standards.

11. Data Protection Impact Assessment (DPIA)

11.1 It is the responsibility of the ANPR Manager to ensure a DPIA is completed prior to any new ANPR fixed sites being commissioned (refer section 3.5) and an annual review of existing sites.

12. Other ANPR Data Sources

12.1 Any consideration to receiving ANPR data from sources other than those owned or operated by the Forces will not be actioned unless approved by the ANPR Manager to ensure compliance to NASPLE.

13. Fault Reporting

13.1 Currently the Forces use the NAS as its operational back-office facility. It carries out the following functionality.

• The roadside NRD captures three packets of data, the colour overview image of the vehicle, the plate patch image of the vehicle's registration number and the textual data containing the time, date, and location expressed in latitude / longitude.

• The National Naming convention for NRD locations are applied within the NAS so that users know instantly the locations of the NRD, particularly for the respective control room staff monitoring alarms. With the advanced functionality in NAS other forces cameras can be used on the borders for dispatcher monitoring of alarms.

• Loaded into the NAS are VOI hotlists that comprise of the following.

1. PNC Act Markers, PNC Lost Stolen

2. Local forces hotlists (VOI) National VOI (Op Tutelage for insurance, No MOT)

3. Bulk hotlists (MIDAS uninsured vehicles, Driver and Vehicle Licensing Agency (DVLA) No Keeper, No Excise Licence)

• All reads transmitted to the Forces ANPR management server for onward transmission to the NAS, all hotlists are matched within the NAS system. If any matches are found an alarm will be generated to any person logged into the NAS dispatcher giving them all the information contained within the VOI hotlist.

• The NAS is linked to PNC; it is called PNC fast track and will carry out a quick time PNC check to validate a VOI alarm and store that data on the individual alarm record.

• The NAS is linked to a Make, Model and Colour (MMC) server utilising data supplied by the DVLA daily. When the NRD passes the registration number to NAS it checks the MMC to find the make, model and colour of vehicle attributed to that registration number. It then stores the data with the read. This is a powerful search tool for research

intelligence and investigation post incident where a victim or witness can only give a make or model of vehicle or colour, this data can be used to search on NAS without a known registration number.

• The read data is stored for one year in the NAS, in line with the ICO guidance on the retention of data.

• There are advanced analytical products available on the NAS for fast time or post incident research for those officers or staff trained and authorised the tools will automatically be added to their profile when trained.

13.2 Password resets cannot be completed by the joint IT helpdesk. Resets are completed by the ANPR Team. All NAS and camera faults must be reported to the ANPR Data Officer(s) who will escalate appropriately to the maintenance team or the Home Office.

Team: Operations Command. Roads Policing Unit.