British Transport Police (BTP)

ANPR System Upgrade

Full Scale Privacy Impact Assessment Report

Document Information	
Document Status & Version	Public Consultation
Version Date	11/08/16
Document Owner	Information Sharing Unit

Document Information	
Document Location	Information Sharing Unit

Table of Contents

Introduction

The Privacy Impact Assessment Process (PIA) is an important tool to ensure that BTP are managing personal information responsibly; only intruding on privacy as far as necessary in order to prevent damage, reduce crime and prosecute offenders.

The PIA process is relevant to initiatives involving the handling of personal information. It enables privacy considerations to be made early on in a project when any identified problems can be easier to resolve.

1. Background

Automatic Number Plate Recognition (ANPR) technology is used to detect, deter and disrupt criminal activity, thus increasing public confidence and perceptions of safety. As a vehicle passes an ANPR camera, its Vehicle Registration Mark (VRM) is read and instantly checked against database records of vehicles of interest. Police officers can intercept and stop a vehicle, check it for evidence and, where necessary, make arrests. A record for all vehicles passing by a camera is stored, including those for vehicles that are not known to be of interest at the time of the read that may in appropriate circumstances be accessed for investigative purposes. The use of ANPR in this way has proved to be important in the detection of many offences, including locating stolen vehicles, tackling uninsured vehicle use and solving cases of terrorism, major and organised crime. It also allows officers' attention to be drawn to offending vehicles whilst allowing law abiding drivers to go about their business unhindered.

2. Project Description

This project is for the purchase of replacement re-deployable equipment to maintain the ANPR system within the BTP jurisdiction. It is recommended that BTP install 3G cameras to replace the present fixed camera system. The new system will allow the BTP to move cameras in light of events or specific intelligence. The project proposal would give greater flexibility of being able to replace cameras for servicing 'as and when' necessary. The maintenance of the equipment would be kept 'in house' and therefore the Force would be self-reliant.

It is also recommended that the Force confirm their intention to convert from the National ANPR Data Centre (NADC) to the new Home Office project National ANPR Service (NAS), in order to fall in line with the remaining Home Office Forces and Law Enforcement Agencies (LEA) to provide a more effective information sharing regime. The NAS will allow all registered users to have direct contact with the system, allowing instant ANPR searches throughout the UK.

3. Anticipated Benefits

- A single national collection of ANPR information to improve delivery
- An increase to the ANPR footprint based on demand and intelligence.

- An improvement in analytical capability, improved information management, scalability and responsiveness.

- Increased adherence to regulatory requirements set by the Information Commissioner's Office and Surveillance Camera Commissioner.

- An increase in detections and disruption of crime. Assisting in bringing offenders to justice and delivering vulnerable persons to a place of safety

- Deployment of ANPR to optimise coverage to address intelligence and security requirements in countering the threat from extremists.

- The current system has been in place for almost ten years and advancements in technology means that this change can be used as an opportunity to improve the performance and functionality of an aging system.

- The on-going provision of data to the National ANPR Data Centre, and subsequently the National ANPR Service in conjunction with other Home Office Forces, will reinforce BTP's intentions to address crime and disorder and be a key participator in national initiatives.

- Through the proposal to upgrade all cameras to 3G re-deployable equipment the Force will not only maintain ANPR coverage at mainline railway stations but also allow more flexibility to incorporate other locations not previously accounted for, if required for specific intelligence led operations or monitoring. This will provide resilience in servicing of equipment effectively, without having an operational impact on BTP staff.

- The provision of new upgraded 3G cameras and the upgrading of software will ensure continual access to the ANPR data shared nationally between other Forces and LEA's. This enables BTP to maintain an effective investigative and intelligence tool locally without having to rely on data requests from other data holders.

4. Legislative Compliance:

Personal information used by British Transport Police (BTP) as a public authority is governed by following legislation and codes of practice.

1) Data Protection Act 1998: BTP processes personal information in accordance with the Act, which exists to ensure the fair and lawful use of personal data and to protect the rights of the data subject. The Act provides exemptions to some of its provisions if complying with them will prejudice the prevention / detection of crime and the apprehension and prosecution of offenders. The Act requires BTP to comply with the following principles when processing personal data:

    - Fairly and lawfully processed.

- Being processed for specified and lawful purposes and not in any manner incompatible with those purposes.
- Adequate, relevant and not excessive.
- Accurate and where necessary, up to date.
- Not kept for longer than is necessary.
- Being processed in accordance with individuals rights.
- Secure.
- Not to be transferred to countries outside the EU ,without adequate protection.

2) Human Rights Act 1998: BTP as a public authority are duty bound to act in compliance with the Act. Article 8 states that everyone has a right to respect for his private and family life, home and correspondence by a public authority. Interference of this right by BTP is not in contravention of the Act if it is in accordance with the law and is necessary, justified and proportionate in a democratic society in the interests of:
   - National security.
   - Public Safety.
   - Prevention of crime and disorder.
   - Protecting the rights and freedoms of others.

3) The information contained within the Force ANPR System will be managed in accordance with the Authorised Professional Practice (APP) on the Management of Police Information (MoPI). The management of information within Force ANPR System will be used throughout its lifecycle to satisfy one of the following MoPI Policing Purposes:
   - Protect life and property.
   - Preserve order.
   - Prevent the commission of offences.
   - Bring offenders to justice.
   - Duty under any statute or common law.

4) The following additional legislation, codes of practice or guidance will be of relevance to the Force ANPR System
   - APP - ANPR
   - Home Office - National ANPR Data Standards
   - Home Office – National ANPR Infrastructure Standards
   - Home Office Surveillance Camera Code of Practice
   - Information Commissioner's Office Data Protection Code of Practice for Surveillance Cameras and Personal Information
   - Protection of Freedoms Act 2012

5. Personal Data Being Processed

The following Personal Data shall be processed as part of this project :

- Vehicle Registration Mark (VRM).
- Vehicle Registration Mark (VRM) –Partial & Misreads.
- Time of VRM capture.
- Location of VRM capture – GPS Coordinates.

- Supporting Imagery – This can include image of vehicle, image of number plate and Geo Tagging.

Whilst a VRM alone does not identify a particular individual, ANPR data will be treated as 'personal data' as defined in Article 2 of the European Directive 95/46/EC.

5.1 Necessity

It is necessary to process all of the above personal data as part of this project as this information is the minimum required to prevent and detect crime. The above information constitutes the information required in the Home Office National ANPR Standards for Policing : Part 1 - Data Standards.

6. Governance

The ANPR System and information held on it is the property of the Chief Constable of British Transport Police and is administered on his behalf by the ANPR Manager.

7. Stakeholders

The following individuals/ organisations will be subject to, or have an interest in, the processing of personal data involved in this project:

- General Public,
- Train Operating Companies,
- Network Rail.

The following internal BTP departments will have an interest in the processing of personal data involved in this project:

- Technology Department,
- Information Security Department,
- Information Governance Department,
- Records Management Department,
- Corporate Risk,
- Force Intelligence Bureau,
- Divisional Intelligence Bureau,
- registered users of the system.

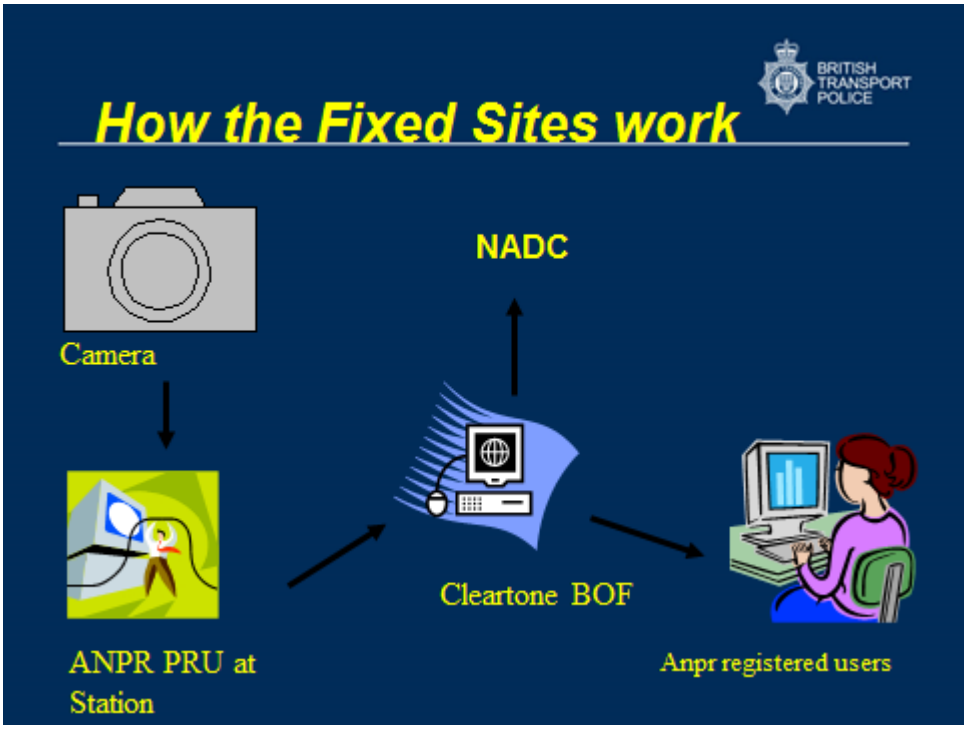
7.1 Recipients

The following external organisations /individuals will have access to, host or receive personal data from BTP as part of this project:

- Home Office National ANPR Service

7.2 Data Flow

The below current data flow is proposed to be amended to movable cameras and the replacement of NADC with the NAS.



7.3 Consultation

This consultation shall be run from 12/08/2016 to 26/08/2016. Please send any comments to informationsharing@btp.pnn.police.uk

The purpose of this consultation is to further identify any potential risks to privacy. Following consultation the relevant mitigations against these privacy risks and what actions are required to be taken shall be identified and this report shall be finalised. After finalisation a public facing copy of this PIA report shall be published on the British Transport Police Website.

8. Privacy Risks Description

Listed below are the identified potential privacy risks resulting from the upgrade of the Force ANPR System.

A) Security of personal information:

The Data Protection Act 1998 requires that 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'. Any loss of personal information or unauthorised access to personal information will be an increased intrusion into that individual's privacy and may well cause them damage or distress. BTP uses the

Government Security Classification (GSC) scheme which provides a consistent framework to identify the sensitivity of information and the appropriate secure handling requirements dependent on that sensitivity.

B) Fair Processing

Unless an exemption applies, the Data Subject is entitled under the Data Protection Act to be notified of the following details when personal data is processed: 1) identity of the data controller, or nominated representative 2) the purpose, or purposes, for which personal data is processed 3) any further information necessary to endure that processing is 'fair'. As this proposal is for ANPR cameras to be located on Train Operating Company property there is potential for confusion amongst the public regarding the ownership of these cameras and the relevant Data Controller.

The Data Protection Act requires that personal information must be fairly and lawfully processed and processed for limited purposes. The use of personal information held within the system should not be a surprise to the data subject, i.e. ANPR cameras are overt and the public expect the police to collect and use personal information to prevent and detect crime, preserve order, and protect the public and property. The 'policing purpose', as set out within Authorised Professional Practice, defines the legitimate purpose of the police and that information used for any of these purposes is policing information. Therefore, a policing purpose will have been satisfied in order for personal information to have been collected, recorded, retained, and shared from the system. Any strategic development of how personal information within the system can be exploited for a policing purpose will be considered by the Information Asset Owner who will have access to expert advice to ensure use of system data remains compatible with a policing purpose and the Data Protection Act. BTP annually notifies the Information Commissioner as to how it will use personal information. BTP also publicises its use of personal information to the public via its internet site.

C) Camera Location assessments and criteria used

ANPR cameras must be located where they will help to detect, deter or disrupt crime. National guidelines state when a police force proposes to install additional ANPR cameras, an assessment must be conducted that demonstrates a clear need, taking account of the following factors:

- national security and counter terrorism,
- serious, organised and major crime,
- local crime,
- community confidence and reassurance, and crime prevention and reduction.

D) Data Sharing

BTP currently shares personal information with partners where it is justified, necessary and proportionate to do so for a policing purpose and in compliance with the Data Protection Act 1998 and the Human Rights Act 1998. Whilst sharing information about an individual's

offending may be felt by that individual to be an intrusion of their privacy and cause them damage or distress; it will be lawful where it is compliant with the aforementioned Acts. The public both accepts and expects the police to share information legitimately with partners for the purposes of preventing and detecting crime and protecting the public. With the aggregation of data within the system a user considering an information sharing request will now have a broader picture of information available to them .Information sharing guidance is available to all BTP staff and expert advice can be sought from BTP's Information Sharing Department.

E) System access

Searches of ANPR data can confirm whether vehicles associated with a known criminal has been in the area at the time of a crime and can dramatically speed up investigations. Unauthorised, or excessive system access could prove a risk to privacy if misuse of data takes place.

F) Handling of data requests from the public – i.e. access to, footage, location of cameras etc.

Under both the Subject Access Provisions of the DPA and requests made under the Freedom of Information Act, the general public are able to request information and personal data held by BTP, subject to the exemptions of the relevant acts. Effective mechanisms must be in place to identify such requests and ensure they are channelled to the relevant departments so that statutory deadlines for response are adhered to.

G) Potential for data to be held longer than is necessary

The Data Protection Act 1998 requires that information is retained for no longer than necessary. Personal information retained in the system for longer than is necessary for a policing purpose could increase the impact on an individual's privacy if that information were acted upon, or disclosed to a partner and acted upon, and resulted in a negative outcome for the subject. BTP manages the retention and deletion of the policing information held within the system by two approaches. The Management of Police Information (MoPI) Retention Schedule sets out retention periods for the holistic retention of a person's information according to whether they poses a risk of harm to the public and if so the level of that risk; the records of the most serious offenders being kept the longest. The National Police Chiefs' Council (NPCC) Retention Schedule is also used to manage the retention of records according to their type. BTP can also be held to account by the data subject who has a right under section 7 of the Data Protection Act 1998 to ask for copies of the information that an organisation holds about them.

H) Data Quality

To comply with the Data Protection Act BTP must ensure that personal information is adequate, accurate and up to date. Any issues with data quality could have an adverse effect on an individual's privacy where, as a direct result, any policing activity or outcome is inappropriate. The system will contain historic data which is necessary for policing and it is widely accepted that information that was accurate at time of recording may not be current many years later. This does not constitute inaccurate information. Data quality issues could include: incorrect data entry, inadequate information being recorded, incorrect linking of records, duplication of records, and incorrect merging of records.

9. Breakdown of Privacy Risks

PRIVACY RISK	RISK TO INDIVIDUAL	ORGANISATIONAL RISK	COMPLIANCE RISK
A) Security of personal information	The loss or theft of personal information is likely to cause the subject damage or distress due to the sensitive nature of police data (offences and offending). Information lost or released outside of the organisation to those who do not have a legitimate reason to process it will infringe the subject's privacy.	Reputational damage to force. ICO enforcement and fines are published. Loss of or reduced confidence in the police about how the police manage information. May be less likely engage with police and share information.	Failure to comply with Principle 7 of the Data Protection Act 1998 (personal information must be secure). If investigated by ICO and found to be in breach of the Act, may be subject to an enforcement notice or fine (maximum £500k). The majority of fines issued by the ICO to date have been as a result of the loss or personal information.
PRIVACY RISK	**RISK TO INDIVIDUAL**	**ORGANISATIONAL RISK**	**COMPLIANCE RISK**
B) Fair Processing	Information captured about offenders and used in differing ways to prevent / detect crime and protect the public is unlikely to infringe the subject's privacy. Any enhancement or evolution of the use of personal data will need to be considered so that it does not constitute unfair processing of an unjustified infringement of privacy.	Reputational damage to force. Loss of or reduced confidence in the police about how the police manage information. May be less likely engage with police and share information.	Failure to comply with Principle 1 and 2 of the Data Protection Act 1998 (personal information must be processed fairly and lawfully and for limited purposes). If investigated by ICO and found to be in breach of the Act, may be subject to an enforcement notice or fine (maximum £500k).

PRIVACY RISK	RISK TO INDIVIDUAL	ORGANISATIONAL RISK	COMPLIANCE RISK
C) Camera Location assessments and criteria used	ANPR may only be deployed at an area which is appropriate and proportionate There needs to be an appropriate balance between the protection of the public with the rights and legitimate expectations of individual privacy.	Potential challenge regarding ANPR placement.	Failure to comply with Home Office National ANPR Standards for Policing : Part 2 – ANPR Infrastructure Standards.
PRIVACY RISK	**RISK TO INDIVIDUAL**	**ORGANISATIONAL RISK**	**COMPLIANCE RISK**
D) Data Sharing	Any excessive / inappropriate disclosure of personal information may cause the subject damage or distress due to the sensitive nature of police data (offences and offending).	Reputational damage to force. Loss of or reduced confidence in the police about how the police manage information. May be less likely to engage with police and share information. Prejudice or undermine a prosecution. Compromise ability to protect the public.	Failure to comply with Principle 1 and 2 of the Data Protection Act 1998 (personal information must be processed fairly and lawfully and for limited purposes). If investigated by ICO and found to be in breach of the Act, may be subject to an enforcement notice or fine (maximum £500k).
PRIVACY RISK	**RISK TO INDIVIDUAL**	**ORGANISATIONAL RISK**	**COMPLIANCE RISK**
E) System access	Improper or unlawful use of the system may result in the subject suffering damage or distress	Failure to retain public confidence may result in a reluctance to engage and share information with the police. If the data subject suffers damage or damage and distress, they are entitled	Improper use by users may breach Principle 1 and 2 of the Data Protection Act 1998 (personal information must be processed fairly and lawfully and for limited purposes). If investigated by ICO

		to compensation if BTP has not taken reasonable steps to comply with the Data Protection Act	and found to be in breach of the Act, may be subject to an enforcement notice or fine (maximum £500k).
PRIVACY RISK	**RISK TO INDIVIDUAL**	**ORGANISATIONAL RISK**	**COMPLIANCE RISK**
F) Handling of data requests from the public	If processes are not effective an individual's legal right to information may be prejudiced.	Failure to retain public confidence may result in a reluctance to engage and share information with the police.	Processing of Subject Access Requests under the Data Protection Act 1998 may take longer due to increased volumes of data. Failure to comply within the statutory 40 day time limit will be in breach of the Act.
PRIVACY RISK	**RISK TO INDIVIDUAL**	**ORGANISATIONAL RISK**	**COMPLIANCE RISK**
G) Potential for data to be held longer than is necessary	Information retained beyond that which is necessary for a policing purpose is likely to infringe of the subjects privacy. If data that is no longer necessary for a policing purpose is disclosed to a 3rd Party it may cause the subject damage or distress that cannot be justified.	Reputational damage to force. Loss of or reduced confidence in the police about how the police manage information retention. May be less likely engage with police and share information. Operational staff may be overwhelmed by the volume of information they see which may result in delays in finding the information they need.	Failure to comply with Principle 5 of the Data Protection Act 1998 (personal information kept no longer than necessary). If investigated by ICO and found to be in breach of the Act, may be subject to an enforcement notice or fine (maximum £500k). Possible challenge in the ECHR (Article 8) that an individual's right to privacy has been unlawfully infringed by keeping personal information longer than is justified,

			necessary and proportionate. Processing of Subject Access Requests under the Data Protection Act 1998 may take longer due to increased volumes of data. Failure to comply within the statutory 40 day time limit will be in breach of the Act.
PRIVACY RISK	**RISK TO INDIVIDUAL**	**ORGANISATIONAL RISK**	**COMPLIANCE RISK**
H) Data Quality	Inaccurate or inadequate data could directly result in an inappropriate course of police action that causes the information subject damage or distress.	Reputational damage to force. Loss of or reduced public confidence in the police. May be less likely to engage with police and share information. Failed prosecution.	Failure to comply with Principle 4 of the Data Protection Act 1998 (personal information must be accurate and up to date). If investigated by ICO and found to be in breach of the Act, may be subject to an enforcement notice or fine (maximum £500k).

10. References and Source Material

During the drafting of this Full Scale PIA Report the following documents and publications have been used for research and as background material :

Hertfordshire Constabulary PIA – ANPR Deployments in Royston (Feb 2014)

Police.uk ANPR information and advice

Metropolitan Police Service ANPR camera sharing with Transport for London for the prevention and detection of crime – Public Consultation Report

Gwent Police – Existing ANPR Network PIA Report

Buckinghamshire County Council ANPR PIA