



**METROPOLITAN
POLICE**

TOTAL POLICING

Protective Marking: Unrestricted		Publication (Y/N): Y
Title: Met Intelligence ANPR Bureau Privacy Impact Assessment		
Summary: Privacy Impact Assessment - Access to ANPR data collected by Transport for London.		
Branch / OCU: Met Intelligence ANPR Bureau		
Date created: 24/9/14	Review date: 01/09/15	Version: V1.0
Author: Det. Supt. Neil Winterbourne		

Contents

1. <u>Introduction</u>	3
2. <u>Public Consultation</u>	6
3. <u>Privacy Impact Screening Questions</u>	9
4. <u>Data Protection and 'Privacy Law' Assessment</u>	10
5. <u>Balanced Risk Assessment</u>	24
6. <u>Implementation of PIA Outcomes Responsibilities</u>	25
7. <u>Conclusion</u>	26
8. <u>Privacy Impact Assessment Sign-off</u>	27

Appendices

i	28
ii	30

1. Introduction

Project Proposal

The Mayor's Crime Manifesto, published in April 2012, made a commitment to make Transport for London (TfL) Automatic Number Plate Recognition (ANPR) data available to the Metropolitan Police Service (MPS) for the purposes of preventing and detecting crime.

TfL collects ANPR data from the central London Congestion Charging Zone (CCZ) and the London-wide Low Emission Zone (LEZ) camera networks and processes it for the purpose of enforcement and traffic monitoring. This data is already transferred to the MPS for the purposes of National Security.

The project proposal is to broaden the purposes for which the MPS can access TfL ANPR data from safeguarding National Security, to include the prevention and detection of crime and the apprehension or prosecution of offenders, in line with the Mayor's Crime Manifesto. Data from TfL cameras will be processed by a specialist unit within the Met Intelligence ANPR Bureau.

The data comprises a continuous feed of alpha numeric characters derived from the vehicle registration marks (VRMs) captured by the TfL ANPR camera system(s). The data transferred to the MPS by TfL, does not include whole of vehicle (overview) photos or number plate (plate patch) photos, albeit that this is collected by TfL and is a component of most Police ANPR data.

The project scope does not include provision for vehicle overview or plate patch images, which would allow the MPS to confirm vehicle details through more thorough investigation. Access to these images may be considered in the future.

There are approximately 1,300 Congestion Charge, LEZ Enforcement and Traffic Monitoring cameras operating 24 hours a day, 7 days a week. This camera infrastructure captures millions of reads from between 650,000 and 700,000 vehicles each day (some vehicles are captured many times because of the particular route they take).

TfL can lawfully retain the ANPR data they collect for their own purposes for only 28 days, while Police retain ANPR data for up to 2 years, to allow for all investigative lines of enquiry to be exhausted. TfL do not have facilities within their own ANPR environment, which are sufficient for and available to the MPS for operational use and nor would this be feasible or effective on logistical or security grounds.

To this end, the only way to harness the ANPR data collected by TfL for longer than 28 days after capture, is to transfer a copy of this data to the MPS where it can be accessed and processed for these purposes.

Project Purpose

The MPS use ANPR technology to prevent and detect crime by targeting criminals through their use of vehicles. The policing objectives associated with ANPR are:

- increasing public confidence and reassurance
- reducing crime and terrorism
- increasing the number of offences detected

- reducing road traffic casualties
- making more efficient use of police resources

This project aims to increase the effectiveness with which ANPR is exploited by the MPS by providing them with the opportunity to consider TfL ANPR data alongside other ANPR data to which the MPS has access.

The case for asserting that access to TfL ANPR data will improve MPS performance is set out at Appendix B in a report entitled “*Operational Rationale for MPS Access to TfL ANPR data*”.

Existing Privacy Design Features and Commitments

The MPS processing of ANPR data is restricted to core policing purposes, which, for the avoidance of any doubt, are defined by the Code of Practice on the Management of Police Information as published 14th November 2005 by the Secretary of State for the Home Department and comprise:

- The protecting of life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice, and
- Any duty or responsibility of the police arising from common or statute law

The Code of Practice further states in paragraphs 4.1.1 – 4.3.1 that:

“...Chief Officers have a duty to obtain and manage information needed for police purposes...[and]...information should be recorded where it is considered that it is necessary for a police purpose...”

It is the intention of the MPS to process the ANPR data transferred to it by TfL in line with the underlying principles set out within the above referenced report at Appendix B.

Public confidence in the ability of the MPS to safeguard personal data and to process it fairly and lawfully is of paramount importance. The results of consultation about this proposal, particularly those directly linked to the Privacy Impact Assessment, will directly inform decisions about how the MPS manages and processes ANPR data transferred to it by TfL.

Document Purpose and Scope

The MPS recognises that this proposal involves making a considerable amount of personal data, regarding the private journeys of individuals travelling around London, available to the MPS. The way in which ANPR data is collected means that such data will be made available to the MPS regardless of whether there is any reason to suppose that the individuals in question might be linked in some way to criminal activity.

The collection process aims to gather and retain the details of all vehicles passing an ANPR camera and it is only at a later stage that it will be discovered whether data about a particular vehicle is of interest to Police in the context of their policing functions.

Any belief that Police can or do only retain data which is, at the time, known to relate to a vehicle that is linked to a criminal is entirely mistaken. This is theoretically achievable but not with any ANPR technology that is currently available. It would also be inconsistent with the use of ANPR as

an investigative tool and mean that a great part of the value of the data was lost almost immediately in relation to data collected by TfL. The consequence would be that the MPS was unable to effectively investigate over a thousand crimes per month.

The essence of the MPS proposal is that it should deal with the access to and retention of TfL ANPR data in a transparent manner that mirrors the way Police deal with ANPR data generated by the Police camera network, subject to the same rules and governance.

It bears noting that once TfL ANPR data is received by Police, the Commissioner is regarded as the Data Controller and the data is regarded as Police data. It will then be treated in line with the policies used to manage all police-held information

The MPS' processing of TfL's ANPR data engages Article 8 of the Human Rights Act 1998. This raises a number of 'privacy' related issues which need to be assessed before implementation and means that the following assessments are required:

- Full Scale Privacy Impact Assessment
- Privacy Law Compliance Check
- Data Protection Act 1998 Compliance Check

This document provides the results of these assessments, including the screening assessments.

Stakeholder Analysis

Through discussion and analysis the following potential stakeholders have been identified:

Stakeholders	Roles and Responsibilities
Transport for London	Data Controllers / Data Providers
Information Commissioner's Office	Provision of guidance and oversight
Mayor's Office for Policing and Crime	MPS Oversight and guidance / Public Consultation support
Greater London Authority	Public Consultation Management
ACPO	Owners of national police policy
Police ICT Company Directorate, Home Office (ex NPIA)	Manage national ANPR Infrastructure on behalf of HMG

Additional consideration has been given to other possible stakeholders, however they are not currently relevant to this stakeholder analysis.

2. Public Consultation

Background

The Metropolitan Police Service (MPS) obtained permission to use its funds for an ANPR project seeking to obtain access to data from TfL ANPR cameras, in July 2013. This comprises a Public Consultation and the installation of road signs.

The project funds supported two distinct stages:

1. *A Public Consultation* - to obtain and show the views of Londoners about the proposed change in MPS use of TfL's ANPR data to solve crime.
2. *Over 300 road signs* - stating 'ANPR used for policing purposes' to be installed in almost every London Borough.

Overview

The Public Consultation ran for an eight-week period from 11 February to 8 April 2014 and was undertaken by the Greater London Authority (GLA) Intelligence section at City Hall. It comprised two core areas of work:

1. Communications to ensure Londoners were aware of the proposal.
2. Give Londoners the opportunity to put forward their views.

The communication process comprised:

- Social media promotion of the ANPR Public Consultation via the front page of the GLA website (Talk London), from the GLA events page and on the MOPAC Twitter feed, directing people to the e-survey.
- Editorial coverage and press releases via London.gov.uk, the MPS public facing webpage and via the MPS Directorate of Media and Communication.
- 92,000 leaflets distributed to community centres, libraries for consumer groups with limited or no internet access and to drivers at petrol stations, garages. The MPS and City Hall also distributed leaflets to different groups. The leaflet gave a link to an e-survey (talk.london.gov.uk/road-cameras) and a telephone number, so a hard copy survey could be sent to members of public.

The questions / statements used to obtain public opinion were:

- *To what extent do you agree or disagree that sharing TfL ANPR camera data with the police makes London safer?*
- *Do you think the police should have access to data collected by these cameras to help them tackle crime?*
- *The Met Police should use modern technology to help them fight crime.*
- *The Mayor should ensure that public sector organisations such as TfL and the Met Police work together and share information to improve efficiency and save money.*
- *Public bodies should share personal data in order to improve services and save tax-payers' money.*
- *If personal data is kept securely and properly accessed and used, increasing the amount the Met Police have access to would make us safer.*

- *The Met Police can be trusted to keep road camera data secure and use it properly.*

Numbers of Londoners consulted

- 562,000 people contacted directly to raise awareness of the Mayor's proposal and seek their views.
- 16,600 hits received on the GLA ANPR Public Consultation page.
- Roundtable discussion chaired by the Deputy Mayor for Policing and Crime with representatives from Civil Liberties groups. These included Liberty80, the National Motorist Action Group, London Councils, Big Brother Watch. It also included Local Authority CCTV and ANPR managers, TfL and MPS ACPO representative, Commander Neil Basu.
- In total, 2,315 responses to the GLA online consultation received.

Results

Eight in ten people supported the Mayor's policy to give the MPS access to TfL's ANPR cameras with the findings grouped under the headings below.

Support for the policy

Across all polling, eight in ten respondents support the Mayor's policy to give the Met police access to TfL's ANPR cameras for crime purposes. Around half of all respondents thought the Met Police already had full access to TfL's camera data. In fact very few thought that the police didn't already have full or partial access to TfL's ANPR data.

Sharing information and working together

Eight in ten Londoners support the sharing of data between public organisations to improve efficiency and the use of technology by the Met Police to improve their service.

83% of respondents agreed that the Mayor should ensure that public organisations such as TfL and the Met Police work together and share information to make them more effective and save money.

Keeping data safe and trust

Eight in ten Londoners think that there must be strict rules in place to protect privacy and stop the Met Police misusing personal data collected by road cameras.

61% of poll respondents were confident that the Met Police already uses technologies like road cameras responsibly, while 12% were not.

Self-selecting consultation respondents were slightly less confident with 49% agreeing and 36% disagreeing that the Met Police could be trusted to keep road camera data safe and use it properly.

Benefits

Respondents do see value in this policy helping the police do their job, solving crime, catching more criminals and deterring criminal activity.

The improved safety was also seen in the context of improving the efficiency of the Met Police by ensuring they were well-equipped with technology and so could save resources such as time and money.

Criticism of the policy

Respondents raised concerns around the level of surveillance in the capital, with particular reference to how proper use and security of the data would be ensured.

Some respondents went further than concern about general security of the data and questioned trust in the Met Police, particularly in light of other occasions, highlighted in the media, where data has been mislaid, misappropriated or misused, and the potential for 'creep' of different uses for this data.

Protecting privacy

It was recognised that steps would be required alongside this proposal to protect Londoners against a surveillance state. As such it was specifically stated that the use of ANPR data will be used to protect London from crime.

All personal data derived from ANPR analysis will be managed in accordance with the Data Protection Act (DPA) and MPS guidelines and policies.

In order to ensure the proposals were in line with public expectations and to identify any issues that might be encountered, or need addressing before the policy was implemented, the Mayor also proposed to undertake a Public Consultation exercise to inform the work.

Data from the Public Consultation is incorporated in the following Privacy Impact Assessment, which addresses privacy issues encountered during this exercise.

2. Privacy Impact Screening Questions

		Yes	No
Q.1	Will the project involve the collection of new information about individuals?	X	
Q.2	Will the project compel individuals to provide information about themselves?		X
Q.3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	X	
Q.4	Will the MPS be using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	X	
Q.5	Does the project involve the MPS using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		X
Q.6	Will the project result in the MPS making decisions or taking action against individuals in ways that can have a significant impact on them?	X	
Q.7	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	X	
Q.8	Will the project require the MPS to contact individuals in ways that they may find intrusive?		X

If the answer to any of the above questions results in a 'yes' then a PIA is required.

Further advice regarding this screening can be obtained via the Information Law and Security Group.

3. Data Protection and 'Privacy Law' Assessment

European Convention of Human Rights:

Article 8: Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The MPS is a public authority, therefore, is subject to a statutory duty under HRA Article 6(1) not to act inconsistently with a Convention right. The relevant Convention right for the purposes of this processing is Article 8(1) of the Convention.

It is the view of the MPS that Article 8(1) provides limited protection to the criminal and it is not intended to bar lawful and proportionate law enforcement activities. It is for this reason that the MPS believes that the interference with the Article 8(1) rights can be justified under Article 8(2). The purpose is the prevention and detection of crime. This falls squarely within one of the permissible bases for interference in Article 8(2), which refers specifically to the prevention of disorder or crime. However, the MPS recognises that for the interference to be justified it would need to be "in accordance with the law" and "necessary in a democratic society", within the meaning of Article 8(2).

1. Does this project / initiative address a Pressing Social Need? If so, outline it here:

The Mayor and the MPS want to ensure that London is the safest big city in the world. One of the ways to do this is to use the best available technology, to cut crime and bring more offenders to justice. ANPR is one of those technologies.

The concept of Pressing Social Need is fundamental to this project as it is a necessary ingredient that must be in place, prior to the Mayor exercising his power to direct TfL to share their ANPR cameras and the data generated with the MPS in connection with general policing.

The new Surveillance Camera Code of Practice outlines the requirement for the use of systems such as ANPR for an appropriate purpose that meets a pressing need. The definition at Chapter 3.1.1 is:

"a legitimate aim and pressing need might include national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health and morals, or the protection of the rights and freedoms of others."

The MPS is of the view that this proposal which seeks access to ANPR data collected by Transport for London, meets the requirements of a pressing social need set out above.

Having access to this data will help to solve crime and have a positive impact on Londoners' quality of life. The MPS view is supported by a Public Consultation carried out by the Greater London Authority (GLA) entitled '*Cutting Crime with Road Cameras*'. This process was conducted from February to April 2014 and showed that 8 in 10 respondents support the Mayors policy for the MPS having access to ANPR data from TfL's cameras to solve crime.

2. Are your actions a proportionate response to the social need?

In reference to the requirement for the processing to be fair and proportionate, it is recognised that there needs to be careful limits both as to the range of individuals within the MPS who will have access to both the ANPR data itself as well as the products of its analysis. To this end, the headline privacy design features for this project are as follows:

Currently TfL data can only be accessed by around 50 officers and staff from the ANPR Bureau. This is the absolute minimum required for operational effectiveness. The search parameters for each inquiry are bespoke, crafted according to the needs of the case and prevailing intelligence. This approach ensures that access to data is filtered for the relevant criteria of each investigation and, more importantly, necessary and proportionate.

Data that has been eliminated from the inquiry is retained within the original database in case further crimes should come to notice but is effectively discarded from any further consideration or processing in connection with an investigation.

For staff who are provided with ANPR account access, older data requires a higher level of authority and is restricted to use in cases of more 'serious' crime. Equally, the threshold for access to data collected by other Police Forces and in the National ANPR Data Centre is set at a higher standard than is required for locally collected data, analysed on the local Force system. It is proposed that access rules for TfL data should track these standards.

Access control is not solely defined by the number of staff afforded access to the IT analysing TfL data. The role of each individual working in the ANPR Bureau and their vetting level is regularly evaluated, to ensure it is appropriate for their role. Other considerations include the physical security of the offices and IT servers.

For approximately 12 months prior to the Public Consultation in 2014, the MPS tested the use of TfL ANPR data in preventing and detecting crime. This proved extremely effective:

- professionalising ANPR analysis to support counter-terrorism (CT) and MPS crime investigations.
- improving intelligence development using ANPR, to target offenders that pose the highest risk to the safety of Londoners.
- trebling the number of investigations supported by ANPR analysis.
- significantly increasing the number of Wanted / Missing offenders arrested who

would not have been found without ANPR analysis.

Digital Policing (DP) conduct an independent audit of the use of TfL data, as provided for within the Section 28 Certificate governing transfer of TfL data to the MPS for national security purposes. Controlled use of this data in support of crime investigations only began in November 2012. DP audits this processing annually, the results of which are subject to an annual report to the Home Office and the Information Commissioner's Office (ICO).

Having access to the data from a network of around 1,300 additional ANPR cameras, evenly spread across London, will improve the MPS ability to access data to solve crime and is a proportionate response to the social need.

Common Law Duty of Confidence:

A breach of confidence will become actionable if:

- the information has the necessary quality of confidence;
- the information was given in circumstances under an obligation of confidence; and
- there was an unauthorised use of the information to the detriment of the confider (the element of detriment is not always necessary).

However, there are certain situations when a breach of confidence is not actionable. Those situations are:

1. If a person has provided consent for the processing of their information.
2. If there is a legal requirement to process the information.
3. If it is in the public interest to process the information.

It is the view of the MPS that points 2 and 3 above are applicable for the reasons already outlined in this PIA.

Data Protection Act 1998

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- a) at least one of the conditions in Schedule 2 is met, and
- b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

For the avoidance of any doubt, this project relies on the following definition of policing purpose as defined by the Code of Practice on the Management of Police Information

published 14th November 2005 by the Secretary of State for the Home Department:

- a) The protecting of life and property
- b) Preserving order
- c) Preventing the commission of offences
- d) Bringing offenders to justice, and
- e) Any duty or responsibility of the police arising from common or statute law

The Code of Practice further states in paragraphs 4.1.1 – 4.3.1 that:

“...Chief Officers have a duty to obtain and manage information needed for police purposes...[and]...information should be recorded where it is considered that it is necessary for a police purpose...”

It is the view of the MPS that the requirement for this processing to be both fair and lawful is met through the Pressing Social Need outlined in this PIA (please refer to the Introduction and Section 1).

Data Protection Act 1998:

Where the processing, by its very nature, may not be considered as fair or lawful, the MPS relies on the following Sections of the Data Protection Act 1998 when processing this information:

Section 29(1):

- (a) The Prevention or Detection of Crime
- (b) The Apprehension or Prosecution of Offenders

Section 29(2):

- (a) Processed for the purpose of discharging statutory functions
- (b) Consist of information obtained for such a purpose from a person, who had it in his possession of any of the purposes mentioned in subsection (1), are exempt from the subject information provisions to the same extent as (Sensitive) personal data processed for any of the purposes mention in that subsection.

It is the MPS' understanding that in the engaging of the above exemption the processing of this data is exempt from:

- The first Data Protection Act Principle (except the need to meet the Conditions in Schedule 2 and 3 of the Act),
- The Subject Access Provisions
- The Non-disclosure Provisions.

Exemption from the Non Disclosure Provisions (by virtue of engaging Section 29(1)(a)(b) & (2)(a)(b))

It is also the understanding of the MPS that by virtue of Section 29(1)(a)(b) & (2)(a)(b), the exemption from the Non-disclosure Provisions allows the Commissioner and his Chief Officer colleagues to share/ disclose with each other information obtained as part of our policing purposes as this processing is exempt from the following:

- The first Data Protection Act Principle (except the need to meet the Conditions in Schedule 2 and 3 of the Act);
- The Second, Third, Fourth and Fifth Data Protection Principles;
- The right to prevent processing likely to cause damage or distress (Section 10); and
- The right to rectification, blocking, erasure or destruction (Sections 14(1) to (3)).

When processing this information, the MPS seeks to rely on the following Schedule 2 and 3 Conditions:

Schedule 2:

Paragraph 5(b): the processing is necessary for the exercise of any functions conferred on any person by or under any enactment.

Paragraph 5(d): the processing is necessary for the exercise of any functions of the public nature exercised in the public interest by any person.

Paragraph 6: the processing is necessary for the purposes of legitimate interests pursued by the data controller, except where the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Schedule 3:

Paragraph 7(1)(b): the processing is necessary for the exercise of any functions conferred on any person by or under any enactment.

Paragraph 10: The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph:

Statutory Instrument 2000/ 417:

1(1) The processing—

- (a) is in the substantial public interest; .
- (b) is necessary for the purposes of the prevention or detection of any unlawful act; and
- (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

(2) In this paragraph, “act” includes a failure to act.

10. The processing is necessary for the exercise of any functions conferred on a constable by any rule of law. The legal framework and existing body of guidance in which the MPS relies is provided by the following:

- ACPO Authorised Professional Practice (APP)
- Management of MPS Intelligence Policy
- MPS Intelligence Strategy
- MPS Intelligence Manual
- ACPO (2005) Guidance on NIM, NIM Codes of Practice & NIM Minimum Standard
- The Data Protection Act 1998
- 2010 Guidance on the Management of Police Information

- The MPS Data Protection Standard Operating Procedures (including international data processing compliance standards)
- The ACPO Data Protection Manual of Guidance
- MPS Information Governance Framework
- MPS Information Management Strategy
- MPS Information Management Policy
- MPS Security Code
- MPS Records Management Manual (including the Review, Retention and Disposal Schedule).

National Guidance

- National ANPR Standards - Parts 1 and 2
- Surveillance Camera Code of Practice (ACPO)
- Procedure for the Development and Review of ANPR Infrastructure
- The use of ANPR by Law Enforcement Agencies

MPS Documents / Policy

- Strategy 2013 - 2017
- MPS ANPR Data Access Policy
- ANPR Strategy 2014-17

1. How will you tell individuals about the use of their (Sensitive) personal data?

The MPS has a mature Information Governance Strategy and Structure in place which incorporates the requirements of the MPS to be open and transparent around the nature in which (sensitive) personal data are to be processed (where possible).

The MPS has a comprehensive Fair Processing Notice (FPN) provided at all Custody Suites and on the MPS internet site. This notice includes full details of how a subject may exercise their Principle 6 rights.

In addition, the 'MPS Publication Scheme' page on the MPS public facing website (www.met.police.uk) outlines how the public can obtain access to information on many subjects including information management, documents and reports about salient issues predominately free and related policies about policing. Importantly this also includes FAQs. The ANPR webpage on the same website provides details of ANPR performance and the ANPR Data Access Policy.

An eight week Public Consultation entitled '*Cutting crime with road cameras*' was run between February and April 2014, to obtain opinion and better understand public concerns about the use of ANPR data for crime purposes. The communication process

comprised:

- Social media promotion of the ANPR Public Consultation via the front page of the GLA website (Talk London), from the GLA events page and on the MOPAC Twitter feed, directing people to the e-survey.
- Editorial coverage and press releases via 'www.London.gov.uk', the MPS public facing webpage and via the MPS Directorate of Media and Communication.
- 92,000 leaflets distributed to community centres, libraries for consumer groups with limited or no internet access and to drivers at petrol stations, garages. The MPS and City Hall also distributed leaflets to different groups. The leaflet gave a link to an e-survey (talk.london.gov.uk/road-cameras) and a telephone number, so a hard copy survey could be sent to members of public.

The MPS will continue to inform Londoners about the use of ANPR to solve crime and to provide transparency via the corporate internet site and local engagement.

2.	Do you need to amend your privacy notices?
----	--

The MPS is content that the existing Fair Processing Notice sufficiently covers the intended processing.

3.	If you are relying on consent to process (Sensitive) personal data, how will this be collected and what will you do if it is withheld or withdrawn?
----	---

No. The reasons for this are:

- 1) Consent can be withdrawn by the data subject at anytime, thus requiring the MPS to delete the data and limiting the scope in which the MPS can fulfil our policing purposes.
- 2) The Commissioner still retains a full copy of the data from TfL's ANPR cameras under the power of the Section 28 DPA Certificate and would still be able to access it lawfully using an exemption provided by Section 29 DPA.
- 3) A policy based on consent would be logistically unworkable by virtue of volume. The capture of Police and TfL ANPR data in London is in the region of 8 million reads a day, involving hundreds of thousands of different vehicles. It is unrealistic to consider that the MPS has sufficient resource to contact this number of people to seek consent.
- 4) Obtaining consent would prejudice the purpose in which the data is collected in the first place.

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

	The intended processing is in line with the purposes outlined above as-well-as those listed within the MPS Fair Processing Notice and our notification with the Information Commissioner's Office : Registration No: Z4888193.
1.	Have you identified potential new purposes as the scope of the project expands?
	No, at this time there is no proposal to widen the scope of this project.
Principle 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	
<p>It is not the intention of the MPS to process exhaustive amounts of personal information on the loose premise that it may be useful now or in the future. This approach would simply grind the Service to a halt by virtue of the eventual need to wade through the vast quantities of data in order to locate the relevant piece of information needed for our purposes. Additionally, the cost to hold data (even using the various cloud solutions) is significant; therefore, the MPS is only interested in processing data that is relevant to our policing purposes.</p> <p>If at any point the data processed is found to be excessive to the purposes of the MPS (i.e. the value of the project in preventing and detecting crimes, for example, is not realised in practice) then this processing will be ceased.</p> <p>All ANPR data processing, including TfL data, has been carefully considered and is subject to annual audit, to ensure that access is made on a case by case basis. This process significantly minimised any risks to both the MPS and TfL, pending the outcome of the Public Consultation and prior to the Mayor considering whether to exercise his powers of social development and grant the MPS permanent access to TfL's ANPR cameras.</p> <p>The 2013 audit of MPS ANPR data use, including TfL, found clear evidence of regular monthly dip sampling of requests by the ANPR Bureau DI to ensure that correct processes are being followed and data is being used proportionately. Annual audit of ANPR data will continue, to ensure compliance with legal and regulatory guidance.</p>	
1	Is the quality of the information good enough for the purposes it is used?
	<p>Yes, this proposal and all current ANPR activity carried out by the MPS is based on the proven value of ANPR analysis and interception in fighting crime. The feed from TfL incorporates the number plate (vehicle registration mark [VRM]) of each vehicle monitored in the Congestion Charge zone, Low Emission zone or by their traffic management cameras.</p> <p>In order to further enhance the quality of this data, the MPS aspires to receive number</p>

plate photos (plate patch) and front of vehicle photos (overview) in the future. There will be significant cost to this project but the Information Commissioner's Office will be supportive because it will allow MPS ANPR operators to make further enquiries and confirm or deny the involvement of a specific vehicle more readily.

2 Which (Sensitive) personal data could you not use, without compromising the needs of the project?

All of the data collected from TfL ANPR cameras is required to ensure that ANPR analysis is effective. Having reviewed the position the MPS is satisfied that our use of personal data is proportionate to the social need.

TfL data is already received and retained to safeguard national security, in line with ACPO policy. MPS retention of ANPR data collected by TfL and transferred to the MPS under authority of a Section 28 DPA Certificate, will be unaffected by this proposal. No additional data will be received or retained and data will continue to be retained in line with the stipulations of the prevailing Section 28 Certificate.

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

The MPS is fully aware of the fear around potential damage and distress to the data subject, the organisation and of third parties if the data processed was inaccurate in any way. This is especially so if the processing of that inaccurate data lead to erroneous decisions being taken. However, MPS decision making in relation to those matters in which the data will be used, does not solely rest with the processing of the data in scope of this project.

ANPR data will compliment a series of diverse data sets to be processed by the MPS, allowing the MPS to fully analyse the circumstances leading up to and following a relevant event. It would be impossible for the MPS to make an informed decision around an act of criminality based on ANPR data alone. Therefore, checks and balances will naturally occur as a result of this holistic approach to both Police enquiries and data processing or analysis.

1 How is the MPS ensuring that (Sensitive) personal data obtained from individuals or other organisations is accurate?

The ANPR data collected by TfL is used to monitor and enforce the Congestion Charge Zone and Low Emission Zones and is subject to internal TfL requirements for accuracy and testing. This is beyond the control of the MPS.

The cameras used by TfL are among the most reliable in accurately capturing number plate details in a range of conditions. The MPS is confident that TfL manage its camera network effectively because it is a major revenue stream for the organisation.

Although not entitled to engineer the TfL ANPR camera network, the MPS is committed to ensuring that the performance is of a high quality and has carried out remote testing. This

ensures that the data received from the cameras continues to be of the highest quality.

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

1	What retention periods are suitable for the (Sensitive) personal data the MPS will be processing?
----------	--

The MPS retains ANPR data for two years, in line with ACPO policy. It is proposed to track any changes to this policy to ensure consistency.

Where data is linked to criminal activity or a prosecution it may be deliberately and separately retained, for such period as is necessary in connection with the specific inquiry or judicial proceedings.

There are requirements to retain certain types of information for lengthy periods, for instance if an ANPR record is positively linked to a person who had committed murder it is quite possible under current regulations that the record will be held for many years.

Where data is retained in contemplation of proceedings, or because it has been preserved for the future investigation of an unsolved crime, it is held with a core archive not as a separate chunk of data out of the reach of ANPR users. Specially retained data is put beyond the scope of routine search and would be subject to a necessity and proportionality test before being made available to a specific inquiry. The conditions of access are incorporated within the MPS data access policy.

2	Are you procuring software that will allow the MPS to delete information in line with our retention periods?
----------	---

The MPS retains all textual ANPR data and Plate Patch data (where given) for up to 2 years but front of vehicle (overview) photos are often deleted at an earlier stage (around 3 months), for reasons of cost and archive storage limitations.

Where prosecution is contemplated, or an inquiry remains unsolved, parcels of data including the overview photo, may be separately and deliberately retained for such period as is required for the completion of inquiries or proceedings, including any appeal.

The current MPS ANPR IT system does not allow for the automatic deletion of data at specific retention periods but a manual process removes data over two years old on a monthly basis.

There is no current plan to procure software that will allow for auto-deletion of ANPR data but this will be considered for the User Requirement of the new MPS ANPR IT system. The conduct of a manual process mitigates the risk of deleting data which is required to be held for a specific purpose.

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

The MPS provides full details regarding how a Data Subject can exercise their Principle 6 Rights within the [MPS Fair Processing Notice](#) and [MPS internet site](#).

The MPS has full and comprehensive policies and local work instructions regarding the [handling of Subject Access Requests \(SARs\)](#).

The MPS shall comply with SARs in accordance with the DPA. There are limited exemptions in which the MPS may exercise should the disclosure of information result in any significant harm. For example, Section 29 of the DPA states that (Sensitive) personal data are exempt from the subject access provisions where the application of those provisions would be likely to prejudice the prevention and detection of crime or the apprehension of offenders. The MPS may use this exemption when responding to subject access requests if we feel that the disclosure of information may prejudice these purposes.

Principle 7

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.

1. Does the project / initiative provide protection against the security risks the MPS has identified?

Yes, the MPS has an ongoing programme of modernisation in respect of its ANPR IT infrastructure and system security. The MPS is continually monitoring, reviewing and updating policies regarding the use and security of ANPR to meet any emerging security risks.

The following document was drafted in support of this project is attached as Appendix B: *Operational Rationale for MPS Access to TfL ANPR data*.

2. What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Access to TfL data will only be available to authorised ANPR staff who have been fully trained and work to clear policies. All access is personally password protected. All use is subject to supervision, spot inspections and a risk-based audit of MPS ANPR Users.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data will only be transferred outside of the UK or EEA where it is in line with our Policing Purposes. For example, if the processing identified a terrorist threat to another country or territory. It is the view of the MPS that it would be proportionate to share this information with our international law enforcement colleagues where this would actively lead to the apprehension of an offender and the location of victims. Please refer to the [MPS Compliance Standard for International Data Processing](#) for further details.

Miscellaneous Considerations

1. Complaint Handling

Complaints about the use of Personal Information in relation to this project should be handled by the MPS Data Protection and Freedom of Information Officer.

The MPS and TfL shall respond to any notices from the Data Subject and the ICO that require the cessation or change in the way data is processed.

The MPS and TfL agree to co-operate with the other party in any complaint or investigation about the use of personal information.

2. Freedom of Information Act 2000 (FoIA)

The MPS shall demonstrate a commitment to openness and transparency regarding this processing, subject to any limitations posed by security or confidentiality requirements.

The MPS is a public authority for the purposes of the FoIA 2000. This means that any information held by the MPS is accessible by the public on written request, subject to certain limited exemptions.

In line with guidance from the ICO, the MPS will place this PIA and other associated documents on our FoIA Publication Scheme, so the public can be aware of how we process (Sensitive) personal data. The only exception to this will be the following:

- Legal Advice

- Commercially Sensitive material
- (Sensitive) Personal Data Pertaining to the Consultation Participants
- Information which would otherwise affect the operations of the MPS and is not in the public's interest to disclose.

All public requests for information should be directed to the MPS Data Protection and Freedom of Information Officer.

5. Balanced Risk Assessment

No	Risk	Likelihood L/M/H	IMPACT L/M/H	Solutions / Mitigations	Residual Risk?	MPS SIRO Sign-Off
1.	There is a risk that the MPS is unable to access TfL ANPR data for crime fighting.	M	H	This PIA and other project actions are working towards the Mayor being invited to exercise his powers of social development (S.30 GLA 1999). If accepted, the Mayor will require TfL to share access to their ANPR cameras and the data feed with the MPS.	Should this project be unsuccessful, leaving the MPS without access to TfL data, there would be a HIGH residual risk for the MPS requiring action.	
2.	There is a risk of a technical failure undermining MPS access to TfL ANPR data.	L	H	TfL will continue to liaise with the MPS about technical issues and routine maintenance that could undermine the data feed from the ANPR cameras.	Continuing engagement between TfL and MPS will minimise residual risks.	
3.	There is a risk of MPS ANPR account holder(s) breaching MPS or ACPO policy, leading either to a breach in DPA principles or ICO guidelines.	L	H	MPS and ACPO ANPR policies are regularly monitored and reviewed to ensure consistency. Serious breaches or issues are reported to the Directorate of Professional Standards. Training in the use of ANPR is ongoing.	ANPR Bureau continually educates system operators to ensure strict compliance with MPS and ACPO policy.	
4.	There is a risk that there will be a loss of public confidence in the MPS use of ANPR data, including TfL.	L	M	A new ANPR Back Office facility (IT system) will offer enhanced facilities for audit, real time tracking and performance reporting.	There needs to be continual engagement with OICs to ensure information applied to ANPR records is regularly updated.	

6. Implementation of PIA Outcomes Responsibilities

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved?

	Action to be taken	Date for completion of actions	Responsibility for action
1.	PIA to be read by critical readers in MPS, TfL and MOPAC.	03/10/14	IS
2.	Final PIA to be submitted to MOPAC with letter from the MPS.	10/10/14	IS
3.	Mayor to consider PIA and 2012 crime manifesto pledge, requiring TfL and the MPS to assume joint responsibility for TfL's ANPR camera system.	TBA	MOPAC (GH)
4.	If acceptable to the Mayor, he exercises the GLA's functions provided by Section 30 Greater London Authority Act 1999 to promote social development, giving the MPS access to TfL's cameras to prevent and detect crime.	TBA	MOPAC (BG?)
Contact point for future privacy concerns			
Met HQ: Information Law and Security Group			

7. Conclusion

There is an overwhelming benefit for the MPS in taking the data from Transport for London (TfL) Congestion Charge and Low Emission Zone ANPR cameras and using it alongside police ANPR data for the investigation of crime.

There are robust rules in place that govern how police manage ANPR data and sufficient safeguards in relation to TfL data, which allow it to be accessed under the same rules and conditions that already apply to police data.

A Public Consultation about MPS use of TfL ANPR data shows high levels of support for police access to TfL data in connection with crime fighting. This consultation also increased transparency and engagement with Londoners which is important in maintaining confidence from the public and regulators alike.


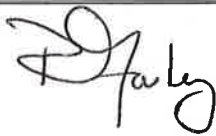
In completing the Public Consultation, the MPS will fall into compliance with the Surveillance Camera Code of Practice and the Data Protection Act by being explicit about the full range of use to which TfL ANPR data will be put in cutting crime. This action will allow the Mayor to consider exercising his power of social development under Section 30 of the Greater London Authority Act and deliver a Mayoral manifesto commitment.

Should the Mayor decide to exercise his powers of social development under section 30 of the Greater London Authority Act, this will have no bearing upon the operation of the Section 28 DPA Certificate, granted by the Secretary of State for the Home Department.

Increased signage around London, to advertise all police use of ANPR, will be a collateral benefit of this project.

No IT infrastructure change or amendment to MPS policy is required to ensure that TfL ANPR data is available for use in crime fighting, although future investment to increase data context and timeliness would both improve the effectiveness of the data and obtain regulatory support.

8. Privacy Impact Assessment Sign-off

1.	Project Sponsor / ACPO Lead
	Sign Below: 
	Name: <u>Richard Maron</u> Position: <u>COMMANDER</u> Date: <u>23rd Decembe 2014</u>
2.	Head of Information Law and Security
	Sign Below: 
	Name: <u>Bob Farley</u> Date: <u>22/12/14</u>

Appendix i

Term	Acronym	Description
Data Controller		Has the same meaning as in section 1(1) of the DPA, that is, the person who determines the manner in which and purposes for which (Sensitive) Personal Data is or is to be processed either alone, jointly or in common with other persons
Data Protection Act 1998	DPA	Includes all codes of practice and subordinate legislation made under the DPA from time to time
Data Subject		Has the same meaning as in section 1(1) of the DPA being an individual who is the subject of (Sensitive) Personal Data
Freedom of Information Act 2000	FOIA	Includes the Environmental Information Regulations 2004 and any other subordinate legislation made under FOIA from time to time as well as all codes of practice
Human Rights Act 1998	HRA	Includes all subordinate legislation made under the HRA from time to time
Information		Any information however held and includes (Sensitive) Personal Data, Non-personal Information and De-personalised Information. May be used interchangeably with 'Data'
Information Commissioner's Office	ICO	The independent regulator appointed by the Crown who is responsible for enforcing the provisions of the DPA and FOIA
Metropolitan Police Service	MPS	The police force for the London metropolis area (excluding the City of London)
Non- personal Information		Information that has never referred to an individual and cannot be connected to an individual.
Notification		The Data Controller's entry in the register maintained by the Information Commissioner pursuant to section 19 of the DPA
Personal Data		Has the same meaning as in section 1(1)(a) to (e) of the DPA, that is, data which relates to a

		living individual, who can be identified from it, or data that can be put together with other information to identify an individual and includes expressions of opinion and intentions.
Process		Has the same meaning as in section 1(1) of the DPA and includes collecting, recording, storing, retrieving, amending or altering, disclosing, deleting, archiving and destroying (Sensitive) Personal Data
Sensitive Personal Data		The eight categories of Personal Data specified in section 2 of the DPA

Appendix ii

Operational Rationale for MPS Access to TfL ANPR data

Overview

The purpose of this report is to articulate the way in which the MPS would utilise TfL ANPR data should it be available for use in the Total War on Crime. It is structured around the current ACPO ANPR strategy, but elaborates on how it applies to or within the Metropolitan Police Service, and makes specific comment where there is a material difference in the nature or scope of that ANPR data as collected by TfL as opposed to that collected by the MPS.

Strategic Vision

The overall aim of Police use of ANPR is to target criminals through their use of the roads by exploiting the full potential of ANPR technology, at national, regional and local levels within the police forces of England and Wales, acting, where appropriate, in partnership with others.

The policing objectives associated with ANPR are:

- Increasing public confidence and reassurance;
- Reducing crime and terrorism;
- Increasing the number of offences detected;
- Reducing road traffic casualties;
- Making more efficient use of police resources.

It is the view of the MPS that each of these Policing objectives will be furthered by securing access to TfL ANPR data. This is based on a rebuttable presumption that, where the value of ANPR data in pursuing these objectives is accepted, access to an increased amount of ANPR data will, through increased scope and granularity tend to increase the effectiveness of Police use of ANPR, and do so without giving rise to significantly increased intrusion.

The nature of general vehicle movements and criminal use of roads, is that both local and exceptional vehicle usage is undertaken by almost all drivers. In particular cases, an ANPR read or series of reads from either local road or arterial road cameras may provide useful information about a particular crime and the linkage of a particular vehicle to it. Over time an accumulation of ANPR reads will reveal potentially important information around lifestyle patterns that may be of use in developing intelligence. In each case the value of ANPR data increases when more detailed information is available and conversely, a thinly spread camera network renders ANPR less useful as an investigative tool.

Values

The MPS signs up fully to active compliance with both the letter and the ethos of ACPO values and applies them in respect of all of its ANPR activity, including that already undertaken using TfL ANPR

data in respect of national security matters. The same values would apply to MPS use of TfL data for Crime purposes. The values are:

ANPR technology will always be used only in accordance with the Law, and in particular with the requirements of the Data Protection Act, Regulation of Investigatory Powers Act, Human Rights Act and Computer Misuse Acts.

While a Vehicle Registration Mark (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.

The continued use of ANPR technology for enforcement purposes is dependent upon maintaining public confidence that the technology is being used correctly and appropriately. Our guidelines will ensure that those deploying and operating ANPR do so whilst recognising and respecting the rights and privacy of individuals.

We will ensure that robust procedures are in place to ensure hotlists and police databases are as accurate as possible and that action is taken over cloned plates whenever these are identified.

We will continue to enforce and renew our procedures to ensure that the risk of misuse of ANPR data by staff is eliminated and that ANPR is only used for legitimate policing purposes.

We will ensure that ANPR data can be deleted and that it is not kept longer than necessary for genuine and justifiable policing purposes.

We will continue to maintain effective access controls, to prevent unauthorised access to ANPR data and to ensure consistency of access to the national database by individual forces.

We will continue to maintain the National ACPO ANPR Standards (NAAS) and ensure that these standards are adhered to.

The Fundamental Principles Of ANPR Data Access And Use

The MPS takes full note of the Home Office principles of privacy and security, and applies them fully, notwithstanding that statutory exemptions from disclosure may apply in relation to some of our use of ANPR data. The principles are:

- *Necessity: collect data for common sense purposes: We collect data to prevent crime and disorder, to protect the public and to safeguard the rights and freedoms of citizens;*

Comment: This must hold true for individual camera deployment decisions but generally this report refers to all cameras collectively. It is rarely the case that an area of London is crime-free, or that vehicle movements in the vicinity will be wholly without capacity to inform the analysis of local crime. This is even more the case in respect of TfL ANPR cameras deployments, which tend to be on main roads and strategically significant roads. There is a significant shortage of police ANPR coverage on the arterial and strategic road network in London. Such roads offer scope for ANPR analysis of both local and pan-London crime. Thus, the MPS would gain immediate and significant operational benefit from access to TfL ANPR data for the purpose of investigating and preventing crime at both local and pan-London level.

- Legality: *ensure compliance with relevant privacy legislation: We ensure that all data is collected, stored and deleted in accordance with the requirements of the Data Protection Act 1998 and the Human Rights Act 1998;*

Comment: The MPS complies with all relevant legislation and Codes of Practice and has a robust audit and DPA infrastructure to both ensure and demonstrate compliance. The MPS would automatically apply the very same regime of governance and safeguards in respect of ANPR data derived from TfL cameras.

- Proportionality: *collect and use data to protect individuals and their communities: We apply a sliding scale so that sensitive data and surveillance techniques are used only for the most serious purposes;*

Comment: The MPS treats all ANPR data as personal information. The MPS only uses ANPR data in the furtherance of Police business, comprising activities that are consistent with the Policing objectives as set out above. The conduct of any inquiry is supervised, to ensure that the inquiry itself is warranted and that all of the investigative measures involved are conducted in a proportionate manner. Additionally, the MPS applies ACPO policy in respect of the authority levels required to conduct inquiries against older data and that which is collected out of its Force area. In cases where it is proposed to use ANPR data in real-time, as part of a surveillance operation, a RIPA authority is required, authorisation being obtained from a Superintendent who is independent of the inquiry.

- Protection: *regulate the people who can hold or access sensitive data, and protect against risk of data loss: We allow only trusted authorities, such as the Police or intelligence agencies, to hold or access sensitive information with tight controls over individual access;*

Comment: Each Police user of ANPR data must apply for creation of a separate ANPR account before they are able to access the system. ANPR operators receive training which includes clear direction about its use. Police officers and staff are subject to a clear disciplinary code in respect of any misconduct, including around their use of MPS IT systems. All data transfers are managed under formal agreements with law enforcement partners, or via ACPO governed transfer to the National ANPR Data Centre. MPS Directorate of Information manages the MPS ANPR infrastructure in line with MPS policy and the DPA. Significant safeguards are in place to prevent unauthorised access to MPS ANPR data.

- Transparency: *make it easy to access your data and to complain: We are open about the data we hold without compromising security and we uphold the rights of anyone who has been unjustly treated;*

Comment: The MPS is an accountable public body that complies fully with the provisions of the Data Protection Act and maintains a department dedicated to ensuring compliance and servicing requests for information under the Act. From time to time, the MPS claims specific exemptions from disclosure in the public interest.

- Scrutiny: *ensure democratic oversight of what we do: We ensure independent scrutiny of what we do from impartial authorities approved by Parliament.*

Comment: The MPS engages appropriately with the Office of the Surveillance Commissioner and the Information Commissioners Office, responding openly to any request for inspections or for information about MPS policies, the conduct of cases or the way in which particular data is managed.

The strategy for data collection & Value for Money

The ACPO vision for developing national ANPR capability until 2020 is set within their document "Building Capability – A Ten Year Strategic Framework". The key components are:

- developing effective operational processes, practices and doctrine, with a vision that "citizens are protected from harm and risk, and the police service is successful in preventing crime and bringing offenders to justice";
- improving the use of information, knowledge and science, with a vision that "citizens are confident that policing makes systematic use of information, knowledge and science";
- continuously improving the delivery of support services, with a vision that "support services for forces are efficient, effective and delivered at the right level";
- increasing the efficiency of service delivery by forces, with a vision that "the police service maximises resources for front-line delivery to meet the needs of citizens".

At national and local level, economic conditions demand efficiency in Police delivery of ANPR services. Sharing the costs and benefits of publicly funded ANPR infrastructure between agencies, as proposed, is likely to become best practice.

When considering the shape of future ANPR data collection in London, it is useful to consider this at three levels:

- The amount and spread of data collection Pan-London
- The amount and spread of data collection in a locality
- The amount of data collection on specified road

The first category is considered by the MPS to be a significant weakness in our current ANPR collection and is highlighted as a risk within the National Counter Terrorism ANPR Strategy. The same is true of the arterial network outside London. Access to TfL ANPR data would go some way towards the short-term mitigation of this problem, though further investment is likely to be necessary in order to manage residual gaps.

There has been great variation in ANPR coverage around London. This is because of the fragmented nature of investment across the Local Authorities in London and between agencies. The consequence is that, in a small number of Boroughs, there is a meaningful ANPR camera network while in the majority there is no significant capability. There is also no coherence between Boroughs. The use of ANPR as a pan-London tool requires consistency, so that vehicles can be tracked effectively rather than being visible in one Borough but invisible in the next. This not only frustrates analysis but more directly curtails the ability of the MPS to manage intervention at a pan-

London level. In a dynamic situation, this compels the MPS towards a practice of inefficient deployment of resources aimed at securing intervention within the scope of often narrowly deployed ANPR coverage, whereas it would be safer and more efficient if Police were able to plan ahead and manage interception across Borough boundaries.

The TfL ANPR camera network spans London far more evenly than the current Police and Local Authority network, in reflection of their pan-London mission. MPS access to data from the TfL camera network would therefore provide widespread and immediate opportunities to manage interception on a large scale. This would tend to improve the success of the MPS in responding to PNC and Hotlist alerts. Where a suspect vehicle can be tracked with greater effectiveness by ANPR it will reduce the instance of high speed pursuit and thereby increase road safety.

There are numerous instances of multiple camera deployments on the same road. The value to TfL is clear because it goes to the heart of traffic management. Where such capability is available to the MPS, it enables conduct of linear interception operations. This style of deployment is central to the development of MPS interception under Operation SPIDER and is inherently more effective and safer than pursuit based interception.

Operation SPIDER will involve the creation of suitable linear camera capability through deliberate procurement and deployment. MPS access to TfL ANPR data for crime purposes would mean that TfL cameras can be incorporated into Operation SPIDER planning. This will mean that less public money is spent on new cameras, while in other areas a combination of existing MPS and TfL cameras will be sufficient to support immediate Operation SPIDER deployments.

Police practice around sharing ANPR data

The Police Service collects and shares ANPR data only for appropriate policing, law enforcement and national security purposes. The sharing of ANPR data by Police is based upon compliance with the National ACPO ANPR Standards (NAAS) document, which specifies the minimum standards to be met by ANPR cameras and systems before they can be connected to the National ANPR Infrastructure. Such connection enables ANPR reads from around the UK to be stored at the National ANPR Data Centre which allows Forces to conduct inquiries against a national data set. In reality, such data rarely goes further than the local Force Back Office Facility (IT).

ANPR data held at NADC is subject to similar access restrictions to those operated in the MPS, except that higher levels of justification and authority are required in order to access it. In order for staff from another Force to access TfL data via the NADC, they would need to convince an Inspector that their inquiry was both necessary and proportionate. It may be important to note that as the NADC is currently configured, the data that it receives is not then sent on to other Forces. Forces post an inquiry to the NADC where it is run against the national data set. The only exception to this sits with SO15 in the MPS, which maintains a national data set for conduct of UK wide national security inquiries.

The infrastructure of data transfer

TfL already pass a full set of their ANPR data to the MPS for use by SO15 in connection with national security. No additional infrastructure will be required either at TfL or between TfL and the MPS in the event that of MPS use of the data is expanded to include crime and general policing.

Any works required at the MPS to manage appropriate access to the data will fall wholly on the MPS to fund and undertake.

It is expected that the requirements and conditions of MPS data transfer and data management for national security purposes would continue apply.

Operational Exploitation

Police exploitation of ANPR data can be divided into three categories:

- Intelligence
- Investigation
- Interception

ANPR data is information that can be analysed to generate useful intelligence or evidence. The relevance of this analysis can then be compared criminal matters. Intelligence is generated proactively, to enhance knowledge about persons or issues of ongoing criminal concern. An investigation however, is conducted to determine certain facts reactively, in response to a crime that has been committed or is ongoing. In ANPR terms, the analytical approach is often very similar whether the product is destined to be intelligence or evidence as there are only so many ways that ANPR data can be manipulated.

Interception is the use of ANPR data, generally by means of comparing it in real-time to intelligence hotlists of the Police National Computer, to trigger immediate Police intervention against a vehicle. A typical example might be that of a stolen vehicle that is subject to a PNC ACT report that passes a Police vehicle with ANPR equipment. The in-car ANPR equipment would be activated by a successful read of the VRM on the stolen car and an immediate interception would ensue.

