METROPOLITAN POLICE TOTAL POLICING

Protective Marking: OFFICIAL	**Publication (Y/N):** Y
Title: **Metropolitan Police Service Retrospective Automatic Number Plate Recognition (ANPR) Privacy Impact Assessment**	
Summary: Privacy Impact Assessment for the use of ANPR in London	
Branch / OCU: SC&O36 ANPR	
Date created: February 2018 **Review date:**	**Version:** 1.0
Author: PS Natasha STRIDE	

Contents

1. Introduction

London attracts criminality at local, regional and national levels, as well as travelling criminals, Organised Crime Groups and Terrorism. Evaluation of the strategic threats to London has confirmed that the risks to national security and the prevalence of organised crime remains. ANPR is an effective and intelligent tool that helps officers to detect, deter and disrupt crime and assists them in protecting vulnerable people

The numbers of people that are, or could be affected by the issues identified within the strategic assessment.
In mid-2015, it was estimated that London's population was 8,673,713 (National Office of Statistics). Anyone residing, working, studying or visiting London would be affected by the categories of strategic threat that are listed above.

Issues around damage/distress caused by crime
Crime can have a very negative impact on local communities and society as a whole. Areas of high crime can become isolated leading to social problems, lack of opportunities and falling house prices. The physical and emotional impact of crime on a victim can be devastating both for those who are harmed and for their families and friends. No matter what the crime or circumstances in which it was committed, it may diminish the victims' sense of control and self-worth.
The effects of terrorism include injuries, death and the psychological trauma of its victims. It can also cause major structural damage to both the immediate and surrounding area of an attack. A terrorist incident will cause short and long-term impact on tourism and the economy. Businesses and industries within London would also be affected resulting in financial loss, and in some cases ruin.

Gang involvement impacts on the health and welfare of the individual, as well as that of his or her family, peers, and community. The numerous consequences stemming from gang involvement can have varying degrees of short and long-term negative outcomes including dropping out of school, unemployment, victimization, drug and alcohol abuse, committing petty and violent crimes, and juvenile convictions. A youth's involvement with a gang (or gangs) leads to an increased likelihood of economic hardship and family problems.

Communities with gang activity are disproportionately affected by theft, negative economic impact, vandalism, assault, gun violence, illegal drug trade and homicide. Members of such communities face heightened fear that they, their families, schools, or businesses, will become victims of theft and/or violence.

How ANPR can assist and how will it be used to address London's problems
ANPR and the exploitation of its data, is a vital tactic that allows Law Enforcement to consider a broad range of options to investigate or intercept vehicle of interest. Such vehicles may be flagged as carrying suspects, vulnerable persons, criminal assets or where the actual vehicle itself is of interest (e.g. crime scene). ANPR has an essential role in proactive policing and Counter Terrorism operations, enabling skilled operatives to assess convoy patterns, routes and time of travel and make general lifestyle assessments richer. ANPR is an effective tool in reactive crime investigation,

allowing law enforcement to research and analyse historic data, furthering enquires relating to people, vehicles and areas of criminal activity.

ANPR is used in proactive policing, cross-border and Counter Terrorism operations, enabling skilled operatives to assess convoy patterns, routes and times of travel and make general lifestyle assessments. Consideration of the strategic threats to London that have confirmed a pressing need for ANPR. The MPS currently has 294 *static* ANPR cameras and the sites for this equipment have been determined using analysis of a number of key factors such as; traffic volume using the road, whether the road is an arterial route, the proximity to crime and criminality hotspots and the levels and patterns of vehicle crime. Each factor has been considered to establish the most appropriate locations for infrastructure taking account of any impact on privacy.

The MPS works with Local Authorities, government departments and businesses operating in London to enhance our ANPR data collection, which will improve investigation capability so that we catch more criminals and reduce crime.

Alternative tactics to ANPR

ANPR is used by MPS officers to meet the challenges of policing London. On a day-to-day basis ANPR is used for a variety of reasons, for example finding vulnerable missing people, locating wanted suspects and stolen vehicles, investigations of all levels of crimes (both primary and secondary investigations) and as part of surveillance operations. There are alternative options that can be used which are more intrusive then ANPR such as use of surveillance teams, roadblocks and Air Support Units. These other tactical responses however are not as effective or as cost efficient as ANPR, nor are they always available especially at short notice. Each camera site has had an analysis to ensure a particular need is met and as such the same or even similar results cannot be expected by the use of other types of systems. The unique nature of ANPR technology and the links between vehicles and all types of crime make it an ideal tool for the purpose required.

Why is ANPR considered to be effective over other forms of investigation?

ANPR offers Police a chance to get a step ahead of crime, exploiting one technology to derive tactical benefits in three different ways; Interception, Intelligence Development and Investigation. It enables Police to investigate crime, manage offenders and intercept vehicles of interest for the purpose of arrest or seizure, or to disrupt crime by denying criminals the use of the roads. It reduces the investigation time taken to identify vehicle-enabled offenders rather than relying on other passive data such as telecoms which can take weeks to retrieve and analyse. ANPR, and the exploitation of its data, is a vital and cost-effective tactic that has broad application to Policing and many other Law enforcement agencies.

A fine example of what can be achieved with the appropriate use of deployable cameras is evidenced by the results of ‘Op Hacienda’, a proactive operation developed by Ealing BOCU in order to target those who commit burglary offences; with dual objectives to arrest nominals involved in residential burglary/Serious Acquisitive Crime (SAC) and to disrupt the activity of Gangs/PPO’s. The operation ran between Oct 2015 and June 2016 was split into 5 phases, each a month long in duration. A key tactic was to utilise ‘deployable’ ANPR cameras, interrogating ANPR data and local intelligence in order to identify the optimal times and locations in which to site equipment alongside bespoke ‘Hotlists’. Officers identified appropriate locations, working in partnership with local CCTV operators and dedicated police resources; this generated strong Command and Control resulting in a substantial 90% intercept rate. All but one of the phases the operation not only achieved its aims

but also exceeded them, reducing residential offences by a substantial 27.5% during December 2015.

How will success be measured?
The Home Office guidance includes a requirement to monitor the ongoing validity of ANPR sites and as such, an annual review process will be put into place, which will allow success to be measured.

As part of ongoing trust and confidence, the Metropolitan Police Service has published the most up to date statistics of Automatic Number Plate Recognition (ANPR) activity and performance on its website, which details:
Number of Successful Interceptions arrests and vehicle seizures
Number of Investigations undertaken by the ANPR Bureau by crime types.
This information follows on from a meeting held in March 2014 with representatives from Civil Liberties groups. The Metropolitan Police Service agreed to provide Automatic Number Plate Recognition (ANPR) Performance data. This is so the public has a fuller understanding about the level of ANPR activity.

Consultation - Local views on ANPR
In 2014, the MPS carried out a Public consultation regarding ANPR. At the time of the consultation, the MPS were proposing to obtain data from cameras owned by Transport for London (TfL). The consultation reached over 8,000 Londoners and concluded that there was overwhelming support for ANPR. Results to the survey are as follows:
8 out of 10 respondents supported the Mayor's policy to give the MPS access to the TfL ANPR cameras.
Around half of all respondents thought that the MPS already had full access to the TfL cameras
8 out of 10 Londoners supported the sharing of data between public organisations to improve efficiency and the use of the technology by the MPS to improve their service.
83% of respondents agreed that the Mayor should ensure that public organisations such as TfL and the MPS work together and share information to make them more effective and save money.
8 out of 10 Londoners think that there must be strict rules in place to protect privacy and stop the MPS misusing personal data collected by road cameras.
61% of Poll respondents were confident that the MPS already uses technologies like road cameras responsibly while 12% were not.
49% of respondents agreed that the MPS could be trusted to keep camera data safe and use it properly whilst 36% did not.
Respondents do see the value in this policy helping the police to 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 MPS by ensuring there were well equipped with technology and so could save resources such as time and money.
Respondents did raise 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 MPS, particularly in light of other times, highlighted in the media, where data has been mislaid, misappropriated or misused, and the potential for the 'creep' of different uses for this data.

It is accepted within the MPS that this consultation has highlighted small areas of public mistrust in the Police and concerns about the level of surveillance in the capital. As a result, the MPS is committed to being more transparent with its use of ANPR. Discussions have taken place with the

Security Camera Commissioner to discuss both Community Engagement and a further Public consultation.

Consultation - Wider views on ANPR

In order to understand the wider societal views of ANPR, public consultations from other Constabularies have been examined along with views from ANPR civil liberty groups. Most notably are the results from surveys by Lancaster Constabulary and Kent Constabulary and views held by the civil liberty group “Big Brother Watch” and the human rights group “Liberty.”

In August 2016, Lancaster Police Constabulary conducted an electronic ANPR consultation survey. In total 4,799 members of the public participated. To summarise the results, the survey concluded that 91% of participants thought that ANPR was used to monitor motoring offences and 75% for investigating crime. 82% would support the increased deployment of ANPR but 43% had concerns for misuse of the information. After an explanation of how the Constabulary uses ANPR technology the number of people supporting ANPR increased to 87% and the number of people who still had concerns reduced to 22%. 82% of participants understood why the location of ANPR cameras were not disclosed and this increased to 87% after an explanation.

In a report detailing police use of ANPR dated March 2013 the civil liberty group “Big Brother Watch” stated: - “The major issues surrounding the use of ANPR involve privacy and proportionality. With a database that holds over 7 billion records there is always going to be scope for data loss or indeed unauthorised access. Perhaps even more worryingly is the potential for this network of cameras to track innocent members of the public for the duration of their journey and then store a record of it.”

On their website the Human Rights Group “Liberty” state - “ANPR, which has expanded enormously without any real public debate or knowledge, raises huge privacy concerns. This technology, originally used to monitor unregistered vehicles, is now routinely being used by the police to locate vehicles (and their owners) that might appear on other – and often dubious – police databases. There is almost no binding regulation about how this technology is to be used, who can be targeted using it, how long images are to be stored for and for what purpose. A database of this magnitude raises real privacy concerns and requires strong regulation.”

It is clear that community engagement is essential to securing public support for ANPR. The public consultation from Lancashire Constabulary highlights how support for ANPR and trust in the Police can be significantly increased when the public are provided with reliable information that addresses their concerns. Misinformation and myths will arise when there is a lack of reliable information available. The MPS is committed in to engaging with the public about this issue via the Safer Neighbourhood Ward Panel meetings and a consideration is being given to a new Public Consultation.

The MPS is currently in the process of updating the Back Office Facility (BOF). The new “MetBoF” system will automatically delete data that is two years old, unlike the previous system, which retained data until it was deleted manually. It is hoped that this will go some way to alleviating concerns from protest groups and the public is general.

Scope of privacy Intrusion

In May 2016 there were 6,158,004 vehicles registered to addresses within London (stats provided by DVLA.) ANPR will identify a vehicle of interest based on the number plate it is displaying and any identification will be followed up by thorough investigative enquiries. Therefore, anyone who owns or drives a vehicle within London or owns or drives a vehicle that enters/leaves London will be affected by the MPS ANPR infrastructure.

Collection/Use/deletion of ANPR Data

Data held both locally and on the NADC may be researched for investigation purposes within clear rules described within National ANPR Standards for Policing (NASP). NASP also includes requirements for audit of access to data.

These rules include 'user defined' permissions to access data based upon a person's role and requirements for prior authorisation of searches based on the type of investigation being undertaken and the length of time that has passed since the collection of data.

Rules and procedures are in place to ensure compliance with the data access and audit requirements of NASP.

ANPR data is retained both locally and nationally for a period of 2 years before it is deleted. Provisions are in place to ensure compliance with the Risk Management and Accreditation Document Set (RMADS) and for securing data accuracy and security in accordance with NASP. The data retention period will from 1st April 2018 further be reduced from 2 years to one year.

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 Social Need? If so, outline it here:**
ANPR is, as outlined in the introduction, a vital tool in the Metropolitan Police Service's fight against crime. It forms an important part of an array of tactics employed to reduce and combat crime and build victim, stakeholder and public confidence. Many crime types (including burglary, robbery, drug trafficking, sexual offences and others) are committed using vehicles, and ANPR is a very effective tool to help bring offenders to justice. It is also a very efficient, safe and cost-effective tactic.	
2.	**Are your actions a proportionate response to the social need?**
The various crime types that ANPR is used to combat, have a major impact on the victims, their families and the community as a whole.	
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.
It must be stressed that there is no intention of the MPS to provide wide access to this data corporately. Nor indeed is it our intention to process this data beyond our core policing purposes. 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 statue 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 as 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 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 him 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 is 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).
- *[Optional Additions: List relevant legal requirements, which necessitate this processing - adds weight to the justifications provided].*

1.	How will you tell individuals about the use of their 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 to this, the MPS publishes copies of the information management related policies we follow, as outlined above. This list is currently subject to a review over the next 6-9 months with a dedicated page on 'Privacy' to be created. This will incorporate all information management policies that the MPS follows on one page, including privacy FAQs, copies of all MPS Information Sharing Agreements, Privacy Impact Assessments, ICO DPA Audits and the MPS Fair Processing Notice (FPN).	
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 personal data, how will this be collected and what will you do if it is withheld or withdrawn?
No. The reasons for this are twofold: 1) Consent can be withdrawn by the data subject at any time, thus requiring the MPS to delete the data and limiting the scope in which the MPS can fulfil our policing purposes. 2) 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 new purposes have been identified at this time.
Principle 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	
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. 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 / initiative in preventing and detecting crimes, for example, is not realised in practice) then this processing will be ceased. The processing will be subject to periodic yearly review in terms of assessing the value that this product plays in enabling the MPS to meet its policing purposes.	
1	**Is the quality of the information good enough for the purposes it is used?**
It is anticipated that the quality of the information is good enough for the purpose for which it is used.	
2	**Which personal data could you not use, without compromising the needs of the project?**
No sensitive data is being used for this project. It will involve the usage of ANPR cameras as outlined in the introduction.	
Principle 4 Personal data shall be accurate and, where necessary, kept up to date.	
The MPS are 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 anyway. This is especially so if the processing of that inaccurate data lead to erroneous decisions being taken. However, the MPS decision making process do not solely rest with the processing of the data in scope for this project / initiative. This data will make up a suite of data that will be processed by the MPS holistically allowing the MPS to fully analyse the circumstances leading up to, and preceding, a criminal event. It would be	

impossible for the MPS to make an informed decision around an act of criminality based on this data alone. Therefore, checks and balances will naturally occur as a result of this holistic approach to data processing / analysing.	
1	**If the MPS are procuring new software does it allow us to amend / delete data when necessary?**
Yes, the existing software, and future software purchases, will allow data to be amended/deleted when necessary.	
2	**How is the MPS ensuring that personal data obtained from individuals or other organisations is accurate?**
Data gathered through ANPR is subject to compliance with the National ANPR Standards for Policing.	
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 personal data the MPS will be processing?**
The information will be retained in line with our Retention, Review and Deletion policy.	
2	**Are you procuring software that will allow the MPS to delete information in line with our retention periods?**
The existing software, and future software purchases, will allow information to be deleted	

in line with retention periods.
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 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?**
The Metropolitan Police Service's ANPR systems are compliant with the National ANPR Standards for Policing (NASP). Data Protection Act Data sets stored and managed securely Deletion/weeding	
2.	**What training and instructions are necessary to ensure that staff know how to operate a new system securely?**
No deployment of new technology will be made without the operating staff being trained and equipped to do so. Training involves MPS guidance on information technology and policing powers, as well as specific training to use the software to interface with the ANPR system.	
Principle 8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and 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.	
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 personal data. The only exception to this will be the following: • Legal Advice • Commercially Sensitive material • 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.

4. Consultation Results

1. Stakeholder Consultation:

1.1 Through discussion and analysis, the following potential stakeholders whose interests may need to be considered have been identified:

Stakeholders	Roles and Responsibilities	Outcomes
Information Commissioner's Office **[Must only be conducted through the Information Law and Security Group]**	*Provision of guidance on completion of the PIA and Pilot Exercise.*	*Advice issued.*
Mayor's Office for Policing and Crime	*Approval to Proceed.*	*Approved*

1.2 Additional consideration has been given to other possible stakeholders; however, they are not currently relevant to this process at this stage.

[Where the initiative is a pilot / trial]

1.3 Full stakeholder consultation will take place post the pilot exercise and will run concurrently alongside the community engagement exercise. The results of which will feature as part of the decision making process as to whether the MPS will proceed or desist with this capability.

2. Public Consultation:

2.1 Consultation as outlines on pages 5-6 (Introduction)

	Method of Consultation	In What Period?	Outcomes
1.	Public ANPR Consultation carried out by MPS	2014	8,000 Londoners reached, with overwhelming support for ANPR technology. (results on page 5)
2.	Electronic ANPR survey by Lancashire Police	August 2016	Participation of 4,799. Again, overwhelming support. (results on page 6)

5. Balanced Risk Assessment

No	Risk	Likelihood L/M/H	IMPACT L/M/H	Solutions / Mitigations	Residual Risk?	MPS SIRO Sign-Off
1.	The deployment of ANPR at a location is not proportionate	L	M	Assessment of 'Pressing Need' supported by a detailed strategic assessment, decisions taken following consultation and consideration of all issues. A robust assessment process for infrastructure provides a proportionate response to the aims of the safeguarding London and taking account of any privacy concerns.		
2.	Individuals not involved in criminal activity consider ANPR as unjustified intrusion on their privacy.	L	M	Transparency in regard to ANPR with provision of information concerning why it is needed, how it is used provide via Internet sites, written communication and trough appropriate		

				signage. Access controls in place in accordance with NASP. Increased awareness of how ANPR is used and the controls in place to prevent misuse will reduce concerns.		
3.	Action taken as a result of ANPR 'hits' from a camera may be seen as disproportionate, or the VRM may have been misread.	M	M	Management controls in place to ensure use is in accordance with NASP. Robust process for managing lists of vehicles of interest to ensure that data for circulated vehicles remains accurate and relevant. Ensure compliance with NASP for system performance. Efficient business process will reduce the likelihood of inaccurate data and compliance with policy on use will ensure that use is proportionate.		

4.	Inappropriate disclosure of data	M	H	Data is only shared and accessed in accordance with NASP. Provisions for monitoring and audit of data access and use in place. Compliance with business rules provides safeguards to prevent misuse and enable the benefits from the development to be realised.		
5.	Excessive data is collected	L	M	ANPR is only deployed where a pressing need has been identified. The continued requirement will be reviewed in accordance with NASP. Retention and disposal of data is in accordance with NASP. Compliance with NASP ensures that data is collected and managed in accordance with agreed national standards. This should be measured against the		

				success criteria identified at the outset, pressing need should also be kept under review		
6.	Data is retained longer than necessary	M	M	Compliance with NASP regarding retention and disposal of data Compliance with NASP ensures that data is collected and managed in accordance with agreed national standards.		
7.	Current Infrastructure is considered disproportionate and subject to complaint to ICO.	M	M	Compliance with national guidance for ANPR. Decisions taken following strategic infrastructure. Assessment taking account of identified privacy concerns identified through timely consultations with appropriate groups and individuals. Decisions regarding the current infrastructure where taken following proper assessment, nonetheless it is		

				recognised that some may disagree with the decisions and the opportunity for review by the ICO is an essential safeguard.		
8.	ICO may determine that infrastructure is inappropriate leading to sanctions.	L	H	Compliance with national guidance of ANPR infrastructure. Decisions taken following strategic assessment taking account of identified privacy concerns identified through timely consultations with appropriate groups and individuals. A robust review process reduces the likelihood of ICO review concluding that the infrastructure at a location is inappropriate.		

6. Implementation of PIA Outcomes Responsibilities

	Action to be taken	Date for completion of actions	Responsibility for action
1.			
2.			
3.			
4.			

Contact point for future privacy concerns
Met HQ: Information Law and Security Group

7. Conclusion

As outlined in the introduction, ANPR technology has a very significant part to play in the fight against crime. Whilst there are some concerns around the potential for intrusion through the cameras and the data obtained from them, it has been shown that there is great public support for the use of this technology, and that there are clear benefits to it. There is National guidance in the shape of the National ANPR Standards for Policing, which provide standards for, amongst other things, the storage, retention and deletion of ANPR data.

8. Privacy Impact Assessment Sign-off

1.	**Project Sponsor / ACPO Lead**
	Sign Below: Name: Position: Date:
2.	**Head of Information Law and Security**
	Sign Below: Name: Bob Farley Date:

Appendices

Appendix A

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 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 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 Personal Data, 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 Personal Data
Sensitive Personal Data		The eight categories of Personal Data specified in section 2 of the DPA

Appendix C: Control page

Distribution list

Recipient	Title	Location

Change control

Version	Date	Authority	Evidence of approval	Record of change