

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



Classification	Official
Suitable for Publication	Yes
Title	DPIA relating to re-integration of the MPS ANPR system with the TfL ANPR system following the expansion of the Ultra-Low Emissions Zone (ULEZ).
Purpose	To consider any privacy issues and mitigate any risks arising
Summary	<p>In order to expand the ULEZ TfL are updating their network infrastructure. This requires a reconfiguration of the network connections with the MPS ANPR system which will impact on the data shared between the 2 organisations.</p> <p>This DPIA assesses the impact of these proposed changes on the privacy of Londoners and concludes that they are a proportionate and necessary measure to maintain the safety and security of the capital.</p>
Author	DCI Phil Darwent
Version	V5
Creating Unit	ANPR Unit -MO2 (Met Intelligence)
Date Created	19/10/2021
Review Date	
CYC Ref	01/DPA/20/000569



Contents

1.	<u>Privacy Impact Screening Questions</u>	Page 2
2.	<u>Introduction</u>	Page 4
3.	<u>Data Protection and 'Privacy Law' Assessment</u>	Page 6
4.	<u>Consultation Results</u>	Page 13
5.	<u>Balanced Risk Assessment</u>	Page 14
6.	<u>Implementation of DPIA Outcomes Responsibilities</u>	Page 15
7.	<u>Conclusion</u>	Page 16
8.	<u>Data Protection Impact Assessment Sign-off</u>	Page 17

Appendices

A	<u>Glossary</u>	Page 18
B	<u>Document Handling Instructions</u>	Page 19
C	<u>Operational Rationale for MPS Access to TfL ANPR data and imagery</u>	Page 21



1. Privacy Impact Screening Questions

		Yes	No
Q.1	Systematic and extensive profiling or automated decision-making to make significant decisions about people.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<i>Systematic monitoring is something that is targeted at broad categories of people rather than specific individuals. It is pre-arranged, organised or methodical, and is carried out as part of a strategy or general plan. Significant decisions may be those which affect entitlement to employment rights such as pay, pensions and allowances, deletion dates for cautions and other criminal records, decisions whether or not to investigate or treat someone as a suspect, or to contact them about their engagement with the police</i>		
Q.2	Large-scale use of special category data or criminal offence data.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<i>The meaning of large scale is not defined in the Act. Factors to consider are the number of individuals whose data will be processed, the variety of different types of data, the volume of data, the duration of the processing, and the geographical extent of the data.</i>		
Q.3	Systematically monitoring or profiling on a large scale, or in a public place.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<i>This would include but is not limited to data captured from surveillance such as CCTV or facial recognition, and ticketing data from events or transport systems.</i>		
Q.4	Using new technology, or novel use of existing technologies.	<input checked="" type="checkbox"/>	
	<i>This will include cases where technology is used in a way which will result in a materially different outcome from the current way of processing data. Consider whether the technology will result in more people being identified, more types of data being captured, data about more people being used, or a larger number of people having access to the data. This is not intended to capture cases simply when a software package is upgraded to a newer version, unless the upgrade will itself produce significantly different results, for example, more thorough evidence review tools.</i>		
Q.5	Processing biometric or genetic data.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	<i>This includes doing anything with DNA samples, DNA profiles and fingerprints</i>		
Q.6	Combine, compare or match data from multiple sources.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<i>This includes discussing individuals at multi-agency panels, as well as using databases and intelligence systems to collate information or wash data-sets against one another. It also includes processing following receipt of data from third parties.</i>		
Q.7	Process personal data in a way which involves tracking individuals' online or offline location or behaviour.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



	<i>This would not extend to individual targeted surveillance authorisations.</i>	<input type="checkbox"/>	<input type="checkbox"/>
Q.8	Process personal data, which could result in a risk of physical harm in the event of a security breach.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<i>Putting security measures in place does not obviate the need to take this risk into account. The risk should be considered in the context of a breach.</i>	<input type="checkbox"/>	<input type="checkbox"/>

If the answer to any of the above questions is 'yes' then a DPIA is required. Further advice regarding this screening can be obtained via the ISSU.

These Privacy Impact Screening questions were completed by A/Insp Michelle Ruane



2. Introduction

The Project

1. **Explain what the project aims to achieve, detailing the benefits to the MPS, the public and other parties.**

Scope of the project

This project is a response to changes made in the TfL ANPR infrastructure as they expand the geographical area of the Ultra-Low Emission Zone (ULEZ).

With the expansion of the ULEZ TfL will be fitting ANPR cameras at approximately 800 new sites around London and upgrading their network infrastructure.

This offers 4 key opportunities and challenges for the MPS:

- 1) Unless the MPS re-configures its connection to the TfL camera infrastructure it will lose access to reads from all current TfL cameras.
- 2) By re-configuring the connection to the TfL network the MPS will receive still images to corroborate the TfL ANPR data that they already take.
- 3) Re-configuring the connection to the newly expanded TfL camera infrastructure will create the opportunity for the MPS to replace some of its more aging and potentially least reliable / accurate camera stock with brand new TfL cameras on a like for like basis.
- 4) Re-configuring the connection to the newly expanded TfL camera infrastructure will also create the opportunity for the MPS to take reads from new additional ULEZ expansion sites if this is deemed proportionate and necessary in the future.

Under this project the MPS is proposing to immediately reconfigure its connection to the TfL ANPR network so that it has access to the imagery which supports the TfL ANPR data it currently receives. This will also create the necessary network connections for the MPS to take reads and imagery from any of the new TfL ULEZ cameras in the future.

- It should be noted that this document will not consider the privacy impact of taking reads from any additional sites as these sites have not yet been identified.
- Any decision to take reads from additional sites in the future will follow a comprehensive, strategic assessment of the wider ANPR infrastructure and be subject to an internal governance process based on a case for operational proportionality and necessity.
- Privacy and equality impact will be assessed as key elements of this process and this document will subsequently be updated accordingly.



Benefits to the MPS, the public and other parties

- **Enhancing the accuracy and evidential value of the MPS ANPR system**

Since 2015 the MPS has taken reads from all TfL ANPR cameras. However, currently the MPS only receives the data not the accompanying visual imagery. This prevents the corroboration or correction of the data significantly limiting its evidential value and overall accuracy.

All ANPR cameras occasionally misread number plates and as a result vehicles are either missed or wrongly identified. This is why the National ANPR Standards for Law Enforcement (NASPLE) sets a 95% accuracy benchmark for ANPR systems.

The accompanying imagery from ANPR cameras allows users to confirm the make, model, colour and VRM of the vehicle in question and corroborate the accuracy of the textual data. Thus any potentially anomalous reads can be checked and errors corrected.

This is valuable in confirming critical individual reads, maintaining overall data accuracy and identifying faults in cameras or the wider infrastructure.

Every uncorrected ANPR misread creates potential for vehicles to evade legitimate law enforcement but also for other innocent vehicles / owners to be brought under suspicion and investigation without justification. As has been highlighted by recent cases in the media, this can lead to further intrusive checks being conducted on individuals, them being contacted by the police, or even arrested. These cases have a negative impact on the individuals involved and the confidence of the wider community in the entire capability.

Camera imagery is also essential for those rare occasions where an ANPR read is to be used in evidence as it will address most of the concerns about the potential for inaccuracy in the data reads.

Additionally, the checking of imagery is a valuable tool in countering the deliberate switching of VRM plates and other attempts to evade detection / identification by the ANPR system.

For the above reasons the capture of imagery alongside ANPR reads is a key requirement of the NASPLE and other regulatory guidance.

The current absence of imagery from the TfL ANPR data was highlighted as a risk at the time of the original 2015 data sharing arrangement and there is a long standing agreement with regulators and the National ANPR data controller that the MPS will endeavour to address this anomaly as soon as possible.

It is important to note that the field, angle and quality of the images is also closely governed by the NASPLE to prevent any additional private information being captured.

- **Retention of access to the current TfL ANPR reads**

Daily, the MPS receives around 8-10 million ANPR reads for the London area and 6-8 million of these come from the TfL system. This therefore makes up 75-80% of the local capability.

Clearly the vast majority of ANPR reads capture vehicles which have no involvement in criminality and these reads will never be viewed or developed. However, in a significant minority of cases the vehicles captured will have been used by those involved in crime and analysis of that data can be invaluable in bringing offenders to justice and protecting the public.

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



The benefits to the public of police use of ANPR have been established over many years. The integrated ANPR system in London helps the MPS to uphold national security, public safety and the economic well-being of the country, prevent disorder and crime, and protect the rights and freedom of others.

The ability to carry out live-time and historic ANPR searches is essential for policing to support operations and investigations in line with current MPS objectives. Having access to ANPR data helps the MPS to solve crime more efficiently / effectively and has a positive impact on the quality of life of residents within London and a wider area.

Some of the key operational benefits of the current MPS ANPR system are:

- The Identification and location of vehicles/offenders involved in criminality.
- Intercepting vehicles involved in criminality and therefore deterring, disrupting and detecting offending.
- Prioritizing the allocation of policing resources and methods of intervention.
- Post incident interrogation of ANPR data to identify offenders and evidential opportunities.

Reads from ANPR cameras have for example played a critical role in the investigations into all of the major terrorist incidents over the last 7 years as well as the wider security plans that keep our Government buildings, tourist sites and other vulnerable locations safe.

At a serious crime level ANPR data is utilised in every serious investigation where the suspect is known or suspected to have travelled by vehicle. It corroborates other digital evidence and it is critical in identifying and locating a large proportion of the most dangerous criminal subjects in London.

In 2020 for example the MPS Central ANPR team received 33,000 requests for assistance from policing., Unfortunately, there is no means to retrospectively review all these investigations to show what value ANPR added to the case.

However, at an anecdotal level it is clear that ANPR intelligence / evidence has played a key role in a significant proportion of recent high profile investigations, and in many of those cases, notably some high profile murder investigations, without the assistance of a comprehensive ANPR system it would have taken significantly longer to identify, apprehend and evidence the movements of the offender.

In all of the above cases, the likelihood of achieving the operational objectives are to a large extent a product of the scale and appropriate focus of the ANPR camera network. The more cameras a vehicle hits the more opportunity there is to link it to a crime, identify a direction of travel and implement a successful intervention.

The loss of the TfL data from the MPS ANPR system would represent a reduction in the wider MPS ANPR capability. While there is no way to retrospectively review what value reads from TfL cameras specifically played in any investigation, given that they make up 75%+ of the network, it will inevitably be significant.

It is also important to note that the TfL ANPR cameras are disproportionately concentrated in central London in areas of high crime, high profile and high vulnerability to terrorism / public disorder. This only goes to amplify the strategic criticality of the TfL reads to the wider MPS capability.

- **Efficient and cost effective maintenance of the MPS ANPR infrastructure**



Much of the MPS ANPR camera infrastructure was fitted before the 2012 London Olympics and is therefore approaching the end of its usable life. During this period there is an inevitable falloff in mechanical reliability and performance which can be seen in daily reporting on the health of the MPS ANPR system.

Furthermore, developments in camera technology mean that even without age related degeneration new models are significantly more accurate and reliable than their predecessors.

As a result the MPS has an ongoing program for replacing its ANPR cameras which is both costly and resource intensive. Each new camera for example costs approximately £5000.

The opportunity to replace some of the end of service MPS cameras with brand new models therefore offers significant potential benefits in further enhancing the reliability and accuracy of the MPS ANPR system whilst saving limited MPS resources for other pressing needs.

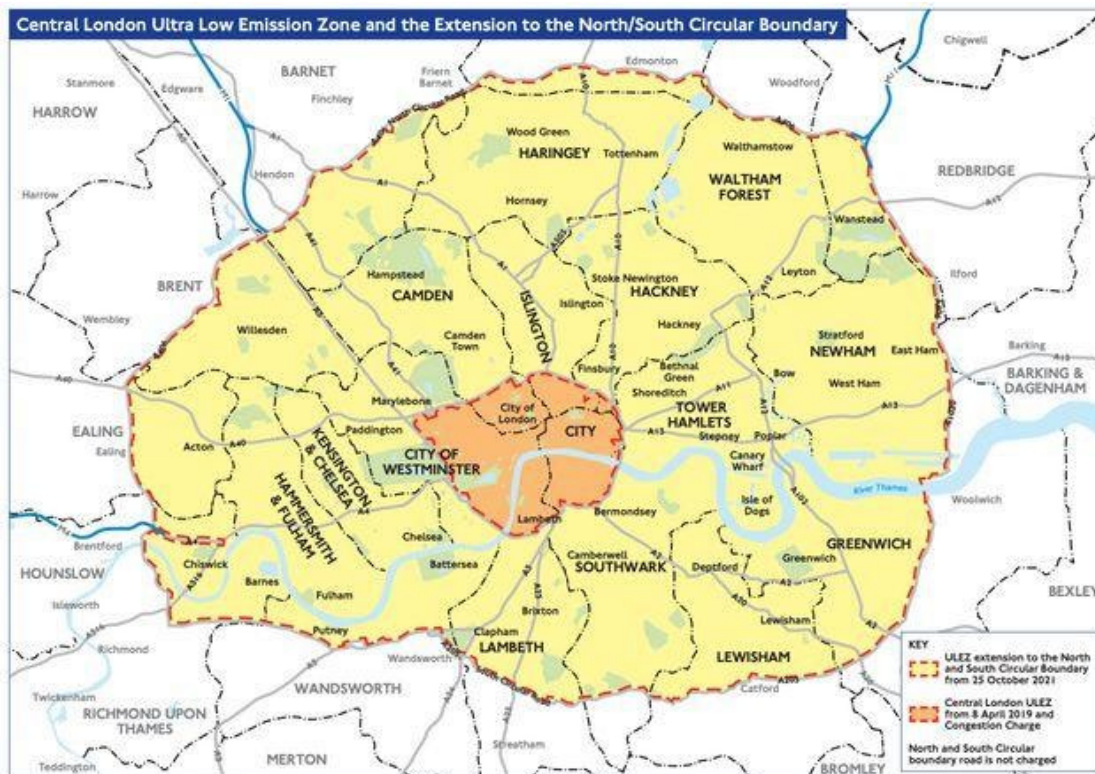
- **The opportunity to efficiently and cost effectively enhance and develop the MPS ANPR Infrastructure in the future**

While the MPS has an established and proven ANPR camera network, it is not without gaps. As much of the camera network has been built by third parties the locations of ANPR cameras does not meet all of the MPS' operational needs. Some parts of London, for example where Local Authorities have not invested in ANPR, are not as well covered as others.

Furthermore, changes in traffic flows and patterns of offending / criminal behavior mean that the locations of cameras become more or less appropriate. Over recent years for example we have seen the unanticipated rise in prominence of drug supply channels between inner London, the Home Counties and rural areas beyond. For this reason the ANPR camera infrastructure remains under constant assessment and review.

The expanded TfL ULEZ incorporates approximately 800 additional camera sites. As the below image shows it also expands coverage into areas of inner and suburban London which were not touched by its predecessor.

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



These are areas that include some significant arterial routes. As such they potentially offer the opportunity to address some of the historic gaps in the MPS ANPR coverage and others which may emerge over time.

While there are no plans to take reads from any additional TfL cameras at present this project ensures that the necessary network integration work is completed to allow for such capability enhancement in the future. Where a suitable proportionality and necessity case is shown, this could provide the ability to further increase crime detections, act more swiftly and obtain supporting evidence in relation to criminal cases.

The sharing of TfL data with the MPS means that data from TfL cameras can be taken at negligible marginal cost. While this can in no way drive decision making it does remove a significant barrier to harnessing new data which is otherwise deemed proportionate and necessary.

While the pressure on public finances only increases it is incumbent on the MPS to consider any opportunity to collaborate with trusted third parties and, make the most efficient use of shared resources. It is clear that the expanded TfL network potentially offers opportunities for such future cost savings.

It is recognised that some have concerns about any potential expansion of the ANPR capability and its impact on privacy and wider civil liberties. These concerns are reflected within the NASPLE and Surveillance Camera Commissioner's requirements for justifying new ANPR infrastructure.

Any proposal to take reads from additional TfL cameras will be treated in the same way as new MPS infrastructure and reviewed through a process which is compliant with these requirements. A case setting out the operational proportionality and necessity will be presented alongside any data protection, privacy or equality considerations and ultimately signed off or rejected by the Commander Intelligence and Covert Policing (or an equivalent peer). Where the case is made out and reads taken, this DPIA and the parallel Equalities Impact Assessment will be updated accordingly.



The decision to share any additional TfL data with the National ANPR System will also be subject to review / authorisation by the NPCC ANPR lead, CC Charlie Hall, with advice from his Data Protection Lead and the combined resources of the ANPR Strategic Infrastructure Board. Again this decision will be based on the application of the principles clearly set out in NASPLE and the Surveillance Camera Commissioner's guidance

Data Governance

The Commissioner and NPCC Lead for ANPR are responsible for National ANPR Data accessed by the MPS. This includes textual data and imagery. The transfer of all ANPR data from TfL to the MPS will continue to be on a Controller to Controller basis.

Overarching 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
- More efficient use of police resources.

This project aims to: secure the MPS ANPR capability by maintaining the current access to TfL ANPR data; increase the accuracy of the ANPR dataset by adding corroborating visual imagery and secure the opportunity to develop the MPS ANPR coverage in the future with reads from additional TfL cameras should it be deemed proportionate and necessary.



2. Briefly describe the new methods that will be applied as part of this processing

TfL currently own and maintain approximately 1,300 Congestion Charge, ULEZ Enforcement and Traffic Monitoring cameras. All of these cameras feed ANPR reads into the MPS ANPR system.

At present the MPS only receive, the textual data, (VRM, Date, time, location) from the TfL data feed. As part of the ULEZ expansion, the wider TfL ANPR infrastructure will also be upgraded and so will the connections to the MPS system. This will allow the MPS to receive visual images showing the number plate and the shape, colour etc of the vehicle itself.

This is of operational importance to confirm that the textual data matches the vehicle that it relates to and decreases the risk of collateral intrusion to the registered keeper/owner by confirming that the vehicle and VRM correctly match. This will also assist in tackling the increasing problem of number plate switching, and other counter ANPR measures, as without a full overview image it is almost impossible to distinguish between a cloned vehicle and one on its true identity.

3. Detail the personal data or special categories of personal data that will be processed (*include the source of the data*)

The MPS treats all ANPR data as personal data. The number plate is personal data and is also described as personally identifiable information, as, when combined with other available data, this can be used to identify a particular individual (ie owner / registered keeper). An ANPR read also captures location details, time and date.

The National ANPR Standards for Policing and Law Enforcement (NASPLE) guidelines, have prescribed limits for image size, therefore it would be extremely unlikely to be of sufficient quality to identify the driver or passengers. There is a possibility that the person's ethnicity or gender could be determined, however this is again extremely unlikely with the cameras TfL use.

These NASPLE guidelines are built into the MPS ANPR system and the pixilation of any image sent to the MetBOF is automatically downgraded to ensure compliance.

The MPS only use ANPR data in the furtherance of police business, comprising activities that are consistent with policing objectives. The conduct of any inquiry is supervised to ensure that the inquiry itself is warranted and that all of the investigative measures involved are proportionate and necessary.

4. Detail how the data will be stored (*include details of review and retention*)

All TfL ANPR data that is shared with the MPS will be stored (in compliance with NASPLE) within the Met Back Office function (METBOF). The MetBOF is the system used to carry out all searches made by MPS ANPR users. A small number of staff in the central ANPR team (approximately 80) can access data for up to twelve months. Other members of staff (approximately 220) from the Local Intelligence Teams, have access to data for up to 90 days. Retention of data on the MetBOF is limited to 12 months unless specifically requested and preserved as part of an investigation or prosecution.

All TfL ANPR data shared with the MPS is also stored within the MPS Analytical Platform Service (APS). This is a stand-alone analytical system which is predominantly used by the ANPR Technical Support Team to monitor the health / accuracy of the wider ANPR system but also to run complex bespoke enquiries across the ANPR dataset which are not possible on the MetBOF. This facility is subject to all the same retention /



deletion protocols as MetBOF however the user group is restricted to only 4 fully trained and qualified individuals within the ANPR Technical Support Team.

The MetBOF and APS are both located in a secure MPS UK based Data Centre.

Any dissemination of data from the ANPR Unit to requesting officers is governed by the Management of Police Information (MOPI). There are occasions where officers request data to be preserved beyond 12 months for the purposes of an ongoing investigation or future prosecution at a later date. Should officers require the data to be kept for longer than 12 months then this is retained within an 'evidence locker' area in the MetBOF. At this time any data in the evidence locker could theoretically be retained for longer than 12 months. Any data within the evidence locker does not have a specific retention period but this is subject to an ongoing review by the ANPR Audit Team which is part of the MPS ANPR Unit.

5. How will the data be processed (*include details of the technology, how access will be limited*)

Access to MetBOF is limited to the MPS Central ANPR Unit and other staff where necessary. Applications for ANPR data are governed by the 7 GDPR principles in ensuring that each request is for a Lawful, Fair and for a Transparent Purpose, Data is relevant to the investigation, Accurate, retention is limited to the period for which it is required, Data Integrity and confidentiality is maintained, and so is Accountability.

The process implemented to assist with achieving these 7 principles requires any request for searches of the system to be formally submitted on a form 5092, outlining the lawful purpose, the reason for the request and how the data will be handled. All requests for service are triaged by a supervisor of Sergeant (or equivalent police staff rank) within MO2 to ensure they fit the submission criteria laid out in the body of the form. In addition to the supervisory verification of each request, routine auditing is conducted to ensure compliance and identify any potential breaches or unusual patterns which would indicate behaviour inconsistent with the 7 principles.

Each request is assigned a unique reference number and the forms are retained on MPS systems for Audit and compliance purposes.

Where an ANPR read is taken from a TfL camera this may also be combined with ANPR reads from other sources, (e.g. MPS or local authority ANPR cameras) Any results/data which relate to the request for searches are entered onto a spreadsheet then passed to the officer/staff member as an intelligence product, along with guidelines on how to protect and manage such intelligence in line with Government Security Classification (GSC). Guidelines are provided on a Form 5090, however this form is not held in the corporate Forms database. If any results are required in an evidential format, then a request must be made separately by the officer/staff member. Any data provided for the purposes of evidence is produced on an MG11 statement.

All staff using the MPS ANPR system are required to complete a Nationally Accredited ANPR specific e-learning package which explains the NASPLE guidelines and other regulations covering the searching, handling, retaining and sharing of ANPR data.

These courses are alongside generic, mandatory MPS data awareness training such as Information and You.

The entire ANPR team are also currently going through a new round of ANPR specific training to support the future use of the National ANPR Service and this incorporates updated sections on Data Protection and management.



Alongside this e-learning there is also an ongoing program of peer to peer training including regular training days at which issues such as Data Protection are covered. System administrators require sight of completion of relevant training courses before accounts are set up.

Police officers and staff are subject to a clear disciplinary code in respect of any misconduct, and this includes the misuse of MPS IT systems. Within the ANPR Unit are staff (ANPR governance team) who are responsible for carrying out regular audits of ANPR data access and usage in line with NASPLE guidelines.

As well as supporting searches across the ANPR data set, the METBOF also automatically generates alerts if a Vehicle designated as a 'Vehicle of Interest' (VOI) or subject to a PNC ACTION report is captured by any linked ANPR camera. Such alerts will be shared with either a restricted group managing a specific operation or a wider user group depending on the sensitivity of the operation, any restrictions placed on the VOI list or the risk level of the PNC ACTION report.

Any user receiving notification of an alert will only receive ANPR data related to that specific vehicle in order to support the activity set out in the operational requirements.

6. How will the data be disposed of (*include the process for assessing when no longer needed*)

All ANPR data held in the METBOF and the APS is deleted automatically once it has gone beyond its 12 month retention period. A further restriction is placed on users' access to data based on permissions which limit access up to 90 days or up to 12 months of data. Data is deleted permanently as per Home Office NASPLE guidelines. This deletion process is an electronic and manual deletion of data. A residual risk remains of electronic software being used to recover deleted data from a disk, however any disks removed from the system are shredded before leaving the hosted environment. Further, restrictions are implemented to prevent users accessing any data beyond 12 months through permissions and controls built into operating systems which prevent users from creating a query which goes beyond 12 months. This also provides protection in the event of any system failures within the automated removal process. This provides compliance with the 5th principle "personal data processed for any purposes shall not be kept for longer than is necessary for that purpose or purposes"

MPS ANPR Users with access to ANPR data and with the required permissions to obtain this data are responsible for deleting data that has been obtained from the system.

The MPS are responsible for all ANPR data held within the APS and as such are responsible for ensuring data is only retained for 12 months. An automated process is currently in place to ensure the system automatically removes data once it has reached the 12 months retention period. Data provided to frontline officers from ANPR requests specifies that they take responsibility for data retention and handling. MPS staff can only access 12 months of ANPR data.

The MetBOF hardware and all associated ANPR data is owned by the MPS. Support services and the application used to query the data is managed by outside contractors. They have responsibility to maintain and service the hardware and the application (MetBOF), however the data is owned and managed by the MPS.



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 their private and family life, their home and their 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 the Human Rights Act (HRA) section 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.

Article 8(1) is a qualified right and does not prohibit lawful and proportionate law enforcement activities which are necessary for the prevention or detection of crime. 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. 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:

What do we mean by a pressing social need in this context?

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

“an aim and pressing need might include national security, public safety, the economic wellbeing 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”

What are the pressing social needs does this project aim to address?

Since July 2005 London has seen numerous terrorist attacks and even more plots foiled by the security services and police.

At the same time statistics have shown persistently high levels of violence and other serious crime. For example, between September 2018 and September 2019 approximately 1 million crimes were reported to the MPS. Around a quarter of these were violence related with further incidences showing high proportions of theft, burglary and vehicle crime.ⁱ



In addition London's transport network, businesses and government buildings have been the target of attack from multiple groups and individuals seeking to disrupt the public in their lawful activity through criminal acts.

All of these incidents have a significant negative impact on the safety, security, confidence, economic opportunities and freedom of Londoners. Prosecuting their perpetrators, and protecting the public from their repetition represents one of the most pressing of social needs in London today.

The MPS is committed to delivering the Police and Crime Plan 2017-2021, set out by MOPAC and working towards a safer city for all Londoners.

Examples of specific threats which the MPS ANPR capability and this project aims to counter include:

Terrorism – London presents an exceptionally attractive target for domestic and international terrorists. There have been multiple terror attacks on central London over recent years which have resulted in significant numbers of deaths and serious injuries. There have also been multiple other similar plots foiled. Many of the perpetrators of these offences travelled into or through London to commit their offences.

Serious and Organised Crime – Much like terrorism the affluent population, tourist traffic and high value businesses of central are a magnet for serious and organised criminals.

Gang controlled drug lines - these spider out across the MPS, into the Home Counties and beyond. The impact of these lines is often seen in associated violence such as shootings/ stabbings and other serious youth violence that poses a risk to both criminal participants and the public at large.

Murder – Premeditated and often involving a level of planning that will see perpetrators move across policing boundaries.

Serious Youth Violence – Often involving rival groups whose focus is territorial. Will involve perpetrators travelling to commit offences. Violence is a key priority in London both for MOPAC and the MPS following an increase in knife and gun crime in the last few years. Gangs are a significant contributor to violence in London and their involvement is clearest when looking at the most serious and harmful level of offences.

Trafficking, Child Exploitation and Modern Slavery – Involves a victim being moved across areas to facilitate criminal activity. For instance, children used to sell drugs on behalf of criminal gangs or trafficked females/males being used as sex slaves

Burglary – Teams of burglars crossing policing boundaries targeting high value commodities such as gold/ jewellery. An example of this is the recently disrupted Chilean crime gangs who were targeting the UK, in particular London

Street Robbery and Snatches – Perpetrators travelling across border to commit offences.

Firearms/ Drugs/ Money – Often moved from one criminal network to another across policing boundaries.



Sexual Offending – Movement of offenders and victims across policing areas. Many offences involve an element of grooming and stalking for which monitoring / evidencing vehicle based movements is critical.

Stolen Vehicles – Often stolen by organised criminal gangs. large numbers of high value vehicles are stolen in London and moved across policing boundaries to be broken up and or shipped abroad.

Unnecessary Road Deaths – Caused by drink and drug driving, disqualified drivers and those using unsafe uninsured vehicles on the road network. ANPR is used to support 'Vision Zero', a mayoral commitment to eliminate all road deaths and serious injuries from London's roads.

Online Child abuse and exploitation - The National Policing Digital Strategy - Digital Data and Technology Strategy 2020-2030 commits to harnessing the power of digital technologies and behaviors to identify the risk of harm and protect the vulnerable in the physical and digital world. This will be achieved by delivering targeted proactive policing approaches and early interventions through the application of digital technology, in this case ANPR data.

How does this project help to address the pressing social need?

As can be seen from the above summary many of the threats posed to Londoners come from offenders who travel into, out of, and across London.

The MPS ANPR system plays a key role in identifying, locating and detaining these offenders. Its use to counter the significant threat from crime and terrorism has been shown to be effective and efficient. Unfortunately there is no reporting mechanism to exactly quantify what role ANPR ultimately played in the 33,000 investigations it supported last year. However, it can be shown that when it is utilised as part of proactive policing operation it delivers significant operational results.

For example, Operation Fastrack, was a 10 week operation run earlier in 2021 to support the MPS' aim of suppressing violence utilising ANPR technology in the pursuit of travelling criminals. It focused on bringing wanted violent offenders to justice swiftly, through the interrogation of ANPR data and other intelligence.

Over the course of the 10 weeks **332** individuals were arrested for **492** separate offences. **129** of the arrests were for violent offences. Alongside these arrests **19** weapons, £539,000 in cash, 14 suspect vehicles, 47 stolen vehicles (worth approx £2 million) and significant quantities of drugs were seized.

The delivery of the objectives set out of for this project is key to maintaining and developing the MPS ANPR capability so that it can continue to counter these threats and meet the associated social needs going forward.

Maintaining access to TFL ANPR data through objective 1 of this project is imperative for the MPS in continuing to protect Londoners. The addition of imagery under objective 2 will assist in these law enforcement aims by addressing some of the current inaccuracy and increasing the probative value of the ANPR data. Furthermore, addressing many of the ANPR misreads through visual corroboration will help the MPS to address the parallel social need of increasing public confidence in policing and its use of technology specifically.



Additionally through objectives 3 and 4 this project will create the potential to harness more of the expanded TFL ANPR network in the future. Responding to changes in the criminal and environmental landscape is imperative for the MPS in meeting the above social needs and, subject to a clear proportionality and necessity case, this project helps to facilitate this.

2. Are your actions/data sharing a proportionate response to the social need this project / initiative has identified?

In assessing the proportionality of the proposed project we need to consider costs and negative impacts of this project against the scale of the social need and the benefits set out above.

What is the impact of the proposed project on the privacy of Londoners and their wider human rights?

ANPR impacts significantly on the privacy of Londoners. As already stated above the drivers of London are captured 8-10 million times per day on the MPS and affiliated ANPR systems. The current TFL cameras alone deliver 6-8 million reads. Every one of these reads captures a small amount of data (location, vehicle number plate, date, time) but, when put together with other data, it can become a powerful tool in monitoring or evidencing the movements of drivers through London.

Given the prevalence of CCTV alongside other state and private sector ANPR systems the public of London have relatively little expectation of privacy when driving their vehicles. The MPS ANPR system is an overt capability. The MPS is entirely transparent about its use of ANPR for law enforcement purposes. Clear signage is in place in the areas where cameras are located and its use is explained within publicly available material such as the recent MPS ANPR survey. Although the exact locations of the cameras is not publicized (to reduce evasion and protect them from vandalism), London's driving public are aware of their existence and the likelihood that their movements will be captured.

Those captured on ANPR will include some who are involved in criminal activity and many more who are not. Whilst ANPR captures and stores a lot of data, the vast majority is never viewed. As discussed below measures are in place which limit the interrogation of the ANPR dataset to lawful policing purposes and therefore it is very unlikely that the millions of innocent reads captured each day will ever be reviewed.

As already highlighted above, the changes outlined in this project will have limited impact on either the nature or the scale of public intrusion from the MPS ANPR system. The inclusion of heavily restricted Imagery alongside the current TFL data will only enhance its accuracy and will not provide significantly more private information. There are no immediate plans to take data from the additional TFL cameras and any future decision to do so will be based on a comprehensive proportionality and necessity case that is subject to a robust internal authorisation process.

When assessing the privacy impact of ANPR use we need to consider other methods of achieving the same operational ends. In practical terms this includes other alternative methods of digital data capture or traditional human surveillance.

Compared to other data capture techniques ANPR is relatively limited in its intrusiveness as only basic geospatial data is captured. Although the scale is great, the information captured does not extend beyond



the location of a vehicle at a particular moment in time. Any other form of digital intelligence capture eg mobile phone data interrogation or CCTV viewing would inevitably intrude more into the subject's privacy.

Human surveillance is hugely limited in its scope by its resource requirements, and is, in many ways, far more intrusive. Humans, and CCTV cameras for that matter, do not have the ability to filter out information which is not directly related to their objective. To create the same retrospective and proactive operational coverage provided by the ANPR system would require thousands of officers working 24 hours a day across London.

The other huge advantage of ANPR over other systems is its refinement. Because the data captured is relatively very limited it can be stored in a much more structured format and searched very easily this makes it far quicker and easier for police to identify information of relevance.

What measures are in place to mitigate the privacy impact of police ANPR usage and this project in particular?

ANPR searching

Within the MPS, searches of the ANPR system are completed by specialist ANPR practitioners providing a service to frontline, specialist crime and counter terrorist investigations teams. These searches add invaluable intelligence (and potentially evidence) where offenders have used the road network.

The search parameters for each ANPR inquiry are bespoke according to the needs of the case and prevailing intelligence. Authorisation for the amount of data requested is dependent on the type and nature of the crime and has to be justified by the requesting officer and approved by a line manager. This approach ensures that access to data and images are limited to the relevant criteria for each request and that they are 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.

Due to technical limitations of the MPS ANPR system, the number of staff with access to the system is restricted. The majority of licenses are taken up by fully trained and appropriately vetted staff working within the ANPR Unit. Additional staff from other departments are provided access dependant on their role, but access is only provided where it is proportionate and necessary for their role and responsibilities. Within this, further restrictions are in place in regards to search capabilities and the number of cameras that staff have access to.

In addition, as an extra security level the MPS ANPR Audit team carry out randomised audit of ANPR usage. Following the NASPLE Audit standards the audit team review 5% of all ANPR searches which are over 90 days and 2% of those under 90 days. These reviews verify that the search meets the operational requirements set out by the investigating officers and is a proportionate and necessary use of the ANPR system.



From the beginning of January 2020 to beginning December 2020 the MPS ANPR team (40 staff) serviced 33,000 requests for such assistance. This in the main was providing investigative support to frontline.

ANPR Alerting

ANPR alerts are created when a vehicle subject to either a Vehicle of Interest list or a PNC ACTION are captured going through an ANPR camera.

Vehicle of Interest lists, (VOI's) are maintained by intelligence professionals. They are compiled from policing intelligence information in order to ensure prolific and known offenders are easily identified. They support proactive intelligence led operations and help to protect Londoners by focusing police attention on the areas of greatest threat. They allow officers to be tasked with operational activity specific to the crime and intelligence picture in their local policing area.

Access to ANPR data in relation to VOI lists is subject to controls which ensure access is provided only where proportionate and necessary to the role. There are a number of security tiers and restrictions linked to the applicant's roles and permissions. These measures enable the MPS to assign access to VOI's and ANPR Data relevant to the applicant's role. All activity in relation to the access provided is captured and subject to Auditing.

ACTION reports are created by operational units in response to a specific operational need eg the driver of a vehicle is wanted for an offence or the vehicle is a crime scene that needs to be forensicated. They are held on the PNC which is directly linked to the MPS ANPR system and the National ANPR System (NAS). They are therefore visible nationally.

Various measures are in place to limit the potential intrusion created by ACTION reports. For example they are graded as High, Medium or Low risk and this dictates how widely any hits are distributed. There is a responsibility on the creator of the report to review the report and update it / remove it once the operational need no longer exists. As a safety measure ACTION reports automatically delete after a predefined period and the MPS Central ANPR team also review the risk grading of reports and their ongoing proportionality.

To provide some perspective on the volume of ANPR alerts, data was reviewed for the 14th October 2020. This showed that there were approximately 15,158 ANPR hits for vehicles of interest and 5976 hits for vehicles subject to PNC ACTION reports ie, for vehicles that have been involved in criminality and require police action. 185 of these hits were for vehicles that are reported stolen.

Overall, ANPR in law enforcement is highly regulated, with clear audit responsibilities incumbent on the police, under the oversight of the ICO and SCC. The MPS regularly reviews and appraises its policies and processes to ensure that users are fully compliant with all relevant law and guidance.

What are the financial and / or any others costs of this project?

While there are significant costs involved in the maintenance and development of the wider ANPR capability the activity covered by this project is almost cost free for the MPS as the bulk of the work is being done by TfL.



The ANPR data received from TfL represents an incredibly cost effective way of delivering operational goals. As already discussed above, other methods of gathering the equivalent data would be significantly more resource intensive and less efficient.

Furthermore, attempting to gather the same ANPR data independent of TfL would be prohibitively expensive. Although there are no detailed costings (as the option has never been actively considered), internal estimates, based on limited data from TfL, suggest that for the MPS to create and maintain an ANPR infrastructure equivalent to the TfL network of ANPR cameras would cost the MPS upwards of £30 Million.

Under these circumstances, and given the other pressure of public sector resources, this limited activity required to maintain the current capability is financially imperative.

How does the public feel about the MPS use of ANPR?

It has also been shown that police use of ANPR has the full support of a substantial majority of the public. The NPCC and Home Office conducted a national Survey in 2021 which showed that 91% of the 92,270 survey respondents support the use of ANPR by UK police forces and 91% also saw the use of ANPR as a benefit to the wider community.

A separate London focused survey conducted by the MPS in support of this DPIA corroborated these findings and showed overwhelming support for the use of ANPR cameras for law enforcement purposes in general (84% of respondents) with over 90% supporting their use in dealing with Counter Terrorism and reducing Crime.

How does the public feel about the MPS using TfL ANPR data for law enforcement purposes?

80% of respondents to the MPS ANPR survey specifically agreed with policing collaborating with partners such as TfL in sharing camera read data, and a similar number agreed to policing having access to the new ULEZ network.

The initial consultation conducted with the ANPR Independent Advisory Group (chaired by the Surveillance Camera Commissioner) raised concerns as to the scale of the potential future expansion if the MPS were to take reads from all of new ULEZ cameras. The group was to a certain extent reassured by the approach being taken by the MPS to any decisions expansion. However they retained some residual concerns about the subsequent governance of these decisions. These concerns have been reflected in the robust assessment and authorisation process set out in this paper.

Overall the public have an expectation that policing will investigate offences and be pro-active in preventing and deterring offending. To effectively do this the MPS must embrace all proportionate and necessary opportunities to harness technology and collaborate with trusted partners. The use of TfL ANPR for lawful policing purposes and everything planned within this project fits within these expectations

What relevant lessons can we take from previous public inquiries and inquests?



Although the below inquiries do not specifically reference ANPR they talk to the expectations on the Police when it comes to exploiting digital opportunities to keep the public safe.

- a. DSD & NBV v The Commissioner of Police of the Metropolis: DSD & NBV brought claims against the MPS for breaches of Article 3 and 8 of the ECHR in relation to the police investigations concerning John Worboys. The MPS was liable to both claimants for a breach of duty imposed upon the police to conduct investigations into particularly severe violent acts in a timely and efficient way. The court concluded that there were multiple and systemic operational failures which individuals and collectively met the test for liability under Article 3. The court also found that as a result of this failures, including the effective linking of criminality, the MPS had effectively caused the sexual assault of NBV by not apprehending Worboys sooner. In the judgment, the court noted:
 - i. (at paragraph 269) *“sexual assault is an offence that is prone to be repeated. Accordingly the possibility that links between different complaints might be identifiable”*
 - ii. (at paragraph 13) *“serious failures in the collection and use of intelligence sources to cross-check complaints to see if there were linkages between them”*
 - iii. (at paragraph 270) *“the Police witnesses that gave evidence were simply not able to account for the fact that connections and links that existed between the various recorded allegations of rape and sexual assault by Worboys were not uncovered earlier”*.
- b. Inquest concerning the deaths of Anthony Walgate, Gabriel Kovari, Daniel Whitworth and Jack Taylor: This matter concerns the murder of four young white males by Stephen Port. Port was arrested on 15 October 2015 for causing the deaths of all four males by administering a poison and subsequently charged and convicted of four counts of murder. He had a fixation with drugging and sexually assaulting youthful looking men and often arranged liaisons with them using gay dating apps such as Grindr. HHJ Sarah Munro QC has been appointed to hear all four inquests, and the missed similarities between the offences has already been a matter of public concern – see for example the Guardian’s report of 10 July 2020 which reports *“Port’s trial highlighted many missed opportunities and potential vulnerabilities in the police investigation. “ ... “The eight-week inquest will examine why the police did not more quickly link four deaths with such striking similarities.”*
- c. Bichard Inquiry: The risk of policing having information but not being able to bring it together, establish the links and realise their significance is a point of relevance arising from the Soham murders. There the Inquiry identified that a lack of a Social Services Information Database that could enable names to be searched and matters to be linked meant the only possibility of a social worker recognising that a particular alleged abuser had a history of contact with Social Services was through memory. The problem with such a system is best illustrated by the fact that Phil Watters was involved in a series of the incidents and appears not to have made the Huntley link between any of them. Whilst in a different context, a similar issue exists with linked offences, where the police have information, are not able to make effective use of it and in this case, the challenge is actually arguably harder as the links can be less obvious and require greater analysis than merely checking against a list of names.

Extrapolating from the above cases it is fair to suggest that the MPS and TFL could be heavily criticized if as a result of not progressing this project TFL did not share data which could, in the hands of the MPS, have directly led to the linking of crimes and the identification and apprehension of some of London’s most high harm offenders, thereby directly preventing further serious offending.



Is the use of ANPR in the current way and the additional measures set out here a proportionate response to the needs of London?

This is ultimately a subjective assessment as to the value placed on privacy relative to supporting the police in countering crime / terrorism and keeping the public safe.

While the value of ANPR to policing is unquestionable, it is recognised by the MPS that, the scale and use of the ANPR capability in London needs to be balanced against the intrusion into the privacy of Londoners and remain proportionate and necessary.

The assessment set out above suggests that the MPS has this balance right and that the public are comfortable with the status quo. Given that the project is focused on maintaining and improving the accuracy of the current capability it is reasonable to extrapolate that this is equally proportionate and necessary.

Clearly the use of the expanded ULEZ network to significantly expand police ANPR coverage in the future would require further proportionality and necessity assessment and this is reflected in the processes that have been set out.

The MPS ANPR team meets regularly with Local Authorities and BCU colleagues to discuss shifting crime problems and strategic planning. Ongoing efforts will be made to determine local community attitudes to crime fighting, with particular emphasis on the use of ANPR. Local authorities and other policing partners will be encouraged to put questions of ANPR usage to local IAGS, and to feed back any significant community sentiments. If strong feelings are identified, Community Impact Assessments and outreach work will be considered.

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 DPIA .

Data Protection Act 2018

Principle 1

(1) Processing of personal data for any of the Law enforcement purposes must be lawful and fair. (2) The processing of personal data for any of the law enforcement purpose is lawful only if and to the extent that it is based on law and either –

- (a) the data subject has given consent to the processing for that purpose, or
- (5a) the processing is strictly necessary for the law enforcement purpose
- (5b) the processing meets at least one of the conditions in Schedule 8.

The core common law principles of policing are outlined below:

- Protecting life and property.
- Preserving order.
- Preventing the commission of offences.
- Bringing offenders to justice.
- National Security

Utilisation of vehicle data and images provide officers with a valuable intelligence for tackling gang related violence, combating crime and safeguarding individuals in London, and operates in furtherance of the core principles.

The Sharing of police information must be linked to a policing purpose. The Management of Police Information (MoPI) Code of Practice defines policing purpose as:

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

A record of the monitoring and issues identified will be used when undertaking and/or conducting an audit.

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 DPIA (please refer to the Introduction and Section 1).

The legal framework and existing body of guidance on which the MPS relies is provided by the following:

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



- **The Data Protection Act 2018 (including Compliance Policy and Guidance)**
- **NPCC Authorised Professional Practice (APP)**
- **NPCC (2005) Guidance on NIM, NIM Guidance and NIM Codes of Practice (2005)**
- **APP Intelligence Management Guidance**
- **2010 Guidance on the Management of Police Information**
- **The APP Data Protection Manual of Guidance**
- **MetSec Code**
- **MPS Information Management Support Pages**
- **National ANPR Standards for Policing & Law Enforcement (NASPLE) 2019**
- **Common Law**

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 and special category data are to be processed (where possible).

The MPS has a comprehensive Privacy Notice. This notice includes full details of how a subject may exercise their right of access to their personal data.

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

The MPS also widely publicised the presence and use of ANPR cameras to drivers in London with signs on road side street furniture. These have been placed in and around key locations fitted with ANPR Cameras to make the public aware of their presence.

The sharing of TFL ANPR data with the MPS for law enforcement purposes is a matter of public record and the supporting MPS and FTL documents are openly available on line.

2. Are you content that the MPS privacy notices covers the intended processing?

If the MPS Privacy Notice will not cover processing after seeking advice ISSU please describe in the box below the additional notice required with a link to it.

I have read the MPS Privacy Notice and I am content that it sufficiently covers the intended processing.

3. Describe below whether you are relying on consent to process personal data, and how this will be collected? If obtaining consent (see explanation below) would prejudice the purpose the data is collected, what legal basis you will be using?

Note: Consent from data subjects, is not always relied upon as a legal basis to process data. This is because consent can be withdrawn by the data subject at any time. If consent is withdrawn, the MPS must delete the data and demonstrate another legal basis.

We are not relying on consent to process personal data.

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The intended processing is in line with the purposes outlined above, those listed in the 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? If the answer to this question is 'yes', then you must seek the advice of the ISSU.

No new purpose has currently been identified for the use of the number plate patch as part of this process. The purpose remains to deter, disrupt and detect offending and criminality, and to safeguard the public.

Principle 3

Personal data shall be adequate, relevant and limited to the necessities of the purposes for which they are processed.

The MPS will not process exhaustive amounts of personal information on the loose premise that it may be useful now or in the future (excessive data collection is also a breach of the DPA 35(2)(b)). This approach would be extremely time and resource intensive, as well as potentially costly. The MPS is only interested in processing data and images that are relevant to a specific investigation or other policing purposes.

The processes and controls set out above ensure that any use of the MPS ANPR system is limited to those required for a legitimate and proportionate purpose. The MPS ANPR Audit Team also monitor usage on an ongoing basis to ensure that correct processes are being followed and data is being used appropriately.

1 Which personal data could you not use, without compromising the needs of the project?

There is no personal data which cannot be used.

Principle 4

Personal data shall be accurate and, where necessary, kept up to date and erased or rectified without delay.

The MPS is mindful of the potential damage and distress to the data subject, the organisation and to third parties if the data processed was inaccurate in anyway. To mitigate this, an ongoing examination of the accuracy and quality of the data must occur throughout the course of the processing.

The changes proposed in this project – specifically through the incorporation or ANPR imagery - will significantly enhance the ability of the MPS to test and verify the accuracy of the ANPR data taken from TfL and facilitate appropriate rectification.

1 If the MPS is procuring new software, does it allow the data to be amended / deleted when necessary? The answer to this question must always be yes. The system should also enable the ability to note that the accuracy of information has been challenged and why.

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



At this time all data will be contained within the current MPS Back Office System and no new software will be necessary. This may change in the future with the introduction of the National ANPR System (NAS) however that system and its use by Law Enforcement agencies is subject to a separate DPIA.

2 How is the MPS ensuring that personal data obtained from individuals or other organisations is accurate?

Any personal data received can be cross checked with MPS police indices which include Crime Recording Information System (CRIS), CRIMINT (MPS intelligence database) and Police National Computer (PNC). Data captured from TfL cameras is a recording of a real time event and as such is an accurate record of what has been captured. Vehicle imagery will enhance the ability to confirm the accuracy of the data gathered, but this will be available when TfL upgrade the relevant cameras.

Principle 5

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

The information will be retained in line with our Retention, Review and Deletion policy, document attached below:



[records-management---retention-review](#)

1 What retention periods are suitable for the personal data the MPS will be processing?

The MPS ANPR system limits search parameters to a 12 month period. All ANPR data including associated images are subject to an automatic 12 months retention period and removed from the system as previously described. If the data returned from a query is required as evidence or required for an ongoing investigation, the data can be saved in the MetBOF "Evidence Locker" and retained under MOPI guidelines. Data retained under MOPI guidelines will be used to verify that the data captured is accurate by checking against the associated images such as plate patches and overviews.

2 Are you procuring software will allow the MPS to delete information in line with the corporate retention policy? (The Answer to this Question must always be Yes.) If you are using current MPS software then it might not be possible to delete see guidance.

The MPS is not procuring new software. The MPS is using the existing system called MetBOF. The number plate images will be deleted from MetBOF automatically when the retention period is met.

Principle 6

1. Personal data shall be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.
2. Appropriate security includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Only MPS officers and ANPR staff have access to the database. Access is limited to officers/staff on the ANPR Unit and other MPS officers/staff who require access for a specific purpose. Any request for access is only authorised where it is necessary and proportionate.

The MPS will share TfL data and imagery with other LEA's to prevent and detect crime.

The MPS has software in place to protect its systems from external attack.

The MPS ANPR databases are fully compliant with Sec 62 DPA logging requirement

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



Safeguards

Safeguards: Archiving:

Personal and special category data shall be processed where the processing is necessary for archiving purposes in the public interest

Not applicable as no data is archived.

Safeguards: sensitive processing:

The processing of personal and special category data is reliant on the consent of the data subject and reliant on a DSA, or reliant on a condition specified in schedule 8.

Sensitive processing is not occurring within this project. The MPS is only processing personally identifiable information ie number plate images.

No conditions in schedule 8 are relied upon.

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 Officer (DPO).

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.

The MPS receives very few FOIA request in relation to its ANPR capability. When it does they tend to relate to individual cases or plans for development of the capability that have been reported in the media. For example a request from a journalist was received earlier this year seeking information on how the MPS proposed to use data from the ULEZ expansion.

When such requests are received the MPS endeavours to respond as openly as possible whilst protecting the privacy of others, sensitive methodology and the wider public interest.

The recent surveys openly published by both the MPS and NPCC included significant detail about how ANPR data is used by policing within the MPS and nationally. This was included to address some of the queries raised in previous FOIA requests.

In line with guidance from the ICO, the MPS will place this DPIA 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.

To exercise any of these rights please contact the Information Rights Unit at:
mpsdataoffice@met.police.uk.

1. Individual Rights

GDPR Recital 1(1) the protection of natural persons in relation to the processing of personal data is a fundamental right. (2) Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

2. *Transfers Outside the European Union (EU)*

GDPR Recital 101 (3) *Personal data transferred from inside the EU to controllers, processors or other recipients outside international organisations (5) can only take place if, the conditions relating to the transfer of personal data are complied with by the controller or processor.*

TfL data or imagery will not be transferred outside of the EEA unless it is to assist in:

- The protecting of life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- National Security



4. Consultation Results

1. Public and stakeholder consultation:

	Date	Method of Consultation	Stakeholder	Outcomes
1.	28 th May 2020	ANPR IAG meeting – Chaired by the Surveillance Camera Commissioner (SCC).	Various – public, regulators, Government Bodies	<p>Various recommendations to ensure that the taking of additional TfL data was based on proportionality and necessity rather than opportunity and cost.</p> <p>This has led to significant changes in the project plans and the incorporation of an additional governance layer before any further cameras are added to the existing infrastructure.</p>
2.	Feb 2021	National ANPR survey	Public	The National ANPR Survey showed overwhelming public support for the use of ANPR for policing. This consultation covered the UK and reported 91% public support for the use of ANPR.
3.	04/06 – 23/07/2021	London Specific ANPR survey to cover sharing of data from TfL and wider ANPR use	Public	<p>Between 4th June and 23rd July 2021 the MPS posted an ANPR Survey across its Social Media platforms and through local BCU leads. This survey explained the police use of ANPR and the collaboration with TfL, also highlighting the potential harnessing of some of the new TfL ULEZ cameras in the future.</p> <p>In total 2537 people completed the survey, 93% of whom are drivers using London roads. There was overwhelming support for the use of ANPR cameras for law enforcement purposes in general (84% of respondents) with over 90% agreeing for their use in dealing with Counter</p>

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



				<p>Terrorism and reducing Crime. 80% of respondents agreed with policing collaborating with partners such as TfL in sharing camera read data, and a similar number agreed to policing having access to the new ULEZ network.</p>
4.	20/07/21	ANPR IAG – Chaired by SCC	Various – public, regulators, Government Bodies	<p>The revised plan for immediate reconfiguration of the network connections to allow for imagery to be taken, followed by a strategic review and potential future incorporation of images and reads from the new ULEZ cameras was presented to the members who were largely appreciative of the change of approach.</p> <p>2 concerns were raised by members of the group.</p> <p>It was suggested that the MPS could still end up with a ‘ring of steal’ and therefore should assess / consult on that basis.</p> <p>The MPS provided further reassurance that this was not the intention and that due consideration would be given to every incremental increase in ANPR infrastructure. All such decision making will be in line with National ANPR standards and SCC’s Principles.</p> <p>Given the potential scale of the increase if the MPS do ultimately take all the reads, it was suggested that it should still consider wider political consultation.</p> <p>This suggestion has been considered on a number of occasions. However, it is the Mayor / MOPAC who ultimately give approval for the sharing of the TFL data. They are sighted on this</p>



				<p>document and other governance measures.</p> <p>As the political / elected body it is for them to address the issue of political consultation before giving their approval. They are also fully accountable through the London Assembly and the various assembly committees.</p> <p>It would not be appropriate for the MPS to bypass normal processes and enter the political debate. Policing has requirements as set out in the SCC principles / NASPLE which govern what they should do in these situations and they are being followed in this case.</p>

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 of technical failure undermining MPS access to TfL ANPR data and imagery	L	H	TfL will continue to liaise with the MPS about technical issues and routine maintenance that could undermine the data feed from ANPR camera.	Low	
2.	MPS data is leaked or accessed by those outside of the organisation.	L	H	The data is held within a data 'warehouse' and is accessed via the Metbof system on Aware. Access is limited to specific officers.	Medium	
3.	Data leaked by officers/staff who	L	H	Appropriate processes are in place to limit access to ANPR data	Low	

TFL ULEZ EXPANSION: SHARING DATA AND IMAGERY WITH THE MPS



	have access to the data			within the MPS to those who require it for a legitimate purpose. All ANPR users in the MPS are trained to ensure they understand their responsibilities. The DPS target corrupt officers and staff.		
4.	Incorrect data handling by MPS officers/staff who have access to the data.	L	H	Training is provided to relevant officers and staff at MO2 to ensure that data is handled correctly.	Low	
5.	There is a risk that there will be a loss of public confidence in the MPS use of ANPR data and imagery including TfL	L	H	Policies and training are in place in regards the use of ANPR data for the relevant policing purposes.	Low	
6	A risk that the access to this additional data is viewed by the public, Stakeholders and other regulatory bodies as disproportionate.	M	H	Public consultation, publicise how this additional data is being used to fight crime and the benefits to local and national communities. Continued assessment of the public's view on the use and access of this data. This will also be mitigated by the robust measures implemented to ensure that any sites/data accessed by the MPS are assessed against the operational need and the proportionality.	Low	



6. Implementation of DPIA Outcomes Responsibilities

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



7 Conclusion

If the data privacy risks which have been identified are not capable of mitigating the initial aims of a project, please detail the course of action to be taken including change of aim, methodology or an abandonment of the project.

The aim of conducting a DPIA is to identify and minimise the data protection risks involved in a project / initiative. The conclusion should describe whether risks and solutions which have been identified will impact what the project sets out to do and result in changes to the initial aims.

The measures proposed in this project are necessary to ensure that the MPS continues to receive TfL ANPR data and maintains the operational effectiveness of its current ANPR capability.

The project will also allow the MPS to capture imagery alongside the textual ANPR data that is currently taken from TfL. This will only enhance the accuracy of the MPS' ANPR data and facilitate its more effective use in intelligence and evidential processes.

Additionally, it will integrate the MPS system with the expanded ULEZ infrastructure at a network level and give the opportunity to take textual data and imagery from additional cameras in the future should an appropriate proportionality and necessity case be made out.

The MPS recognises that any significant increase in the ANPR camera network needs to be fully justified and therefore any future decision to take data from these cameras will be subject to a robust internal review and authorisation process.

There are robust rules and safeguards in place that govern how the MPS manages ANPR data from TfL (or any other source) and ensures that it is only accessed, reviewed and shared when it is necessary and appropriate.

Public consultations about MPS use of ANPR continues to show high levels of support for police access to TfL data and images. There is no reason to believe that this won't continue to be the case in the future if data from any additional cameras is added.


There are no other practical or less intrusive means to achieve the objectives set out for this program. It represents a proportionate and necessary response in addressing a pressing social need.



8. Data Protection Impact Assessment Sign-off

1.	Project Sponsor
2.	Head of Information Law and Security

Sign Below:



Name: Fiona Mallon Position: A/Commander
Date: 16/11/21

I have reviewed this DPIA which speaks to an existing processing activity, namely the collection, storage and internal sharing of ANPR data from a network of cameras across London. In this specific case it refers to cameras owned and operated by transport for London, which are then fed into the MPS. The newly created Ultra Low Emission Zone is 'policed' by TFL using an expanded camera network, and whilst the use of these cameras is evidently an opportunity for the MPS to consider, their use is not considered within the DPIA. However, the production of this DPIA has been triggered by that new development insofar as that in order to sustain the current network, there is the need to undertake some 'engineered' reconfiguration of data feeds. This will ensure that should the MPS wish to capitalise on the expanded camera network at some time in the future, this is made possible. **Any expansion of the camera network would need a full assessment of the privacy implications through a refreshed DPIA.**

This DPIA does consider a further benefit of this data feed work, insofar as it will become possible for the MPS to receive imagery obtained from cameras of a deliberately low resolution quality. This will enable confirmation that the index mark, vehicle type and colour match those which are already held on the DVLA database. This is not the capture of new and revelatory information, but data which is most likely to assist in ensuring that innocent individuals are not intruded upon, where for example their index number has been 'cloned' and put to use on another vehicle in the hands of criminals. In essence this is not more intrusive, but in the view of the author, making the use of ANPR data less intrusive. The low quality resolution is deliberately employed to reduce any likelihood that a recognisable image of a driver or passenger will be captured. As a result it is not envisaged that special category data will be captured and therefore sensitive processing.

ANPR does not directly identify a single individual, albeit that index marks link 'keepers' to vehicles. Keepers are expected in law to be able to account for who is using a vehicle on a road at any given time and to be able to provide those details to police. Thus it is clearly arguable that ANPR data provides personal information in respect of identifiable individuals including the time that they were at a particular place, the direction they were travelling; and, where data is linked to other cameras; the extent of a journey and locations visited etc. The vast majority of road users are law abiding persons, going about their daily business, and therefore the routine collection of their data is evidently something which must be weighed in the balance and justified



against the objective policing purposes. The public are used to being captured routinely by CCTV as they go about their business in public places, however they are largely anonymous in this regard. That is not so in the case of ANPR if the police choose to identify a keeper through the use of PNC. It might however be argued that motorists enjoy a diminished right of privacy by virtue of specific legislation, notably the Road Traffic Act. Drivers of motor vehicles must be properly licensed to use the road and police are empowered to stop any driver for the purposes of confirming the driver has a license. Notwithstanding and to ensure that innocent motorists are not unnecessarily intruded upon, the MPS employs the application of a threshold test in the form of form 5092, where the lawful purposes must be justified. Furthermore, there is an audit process to ensure that standards are properly maintained and do not inappropriately drift to a lower threshold. In the round the MPS may also draw support from the findings of public surveys which show strong support for the Police Use of ANPR technologies.

I note within this DPIA that work is being progressed to ensure that appropriate retention periods are set for ANPR reads that have been held within the evidence locker and perhaps more importantly to ensure that when no longer required that data is properly deleted. Whilst this is undoubtedly a minor subset of all data processed through ANPR, the impact on individuals should be assessed properly from a privacy perspective and **I therefore recommend that the scale of the issue and therefore risk is more formally set out such that the Information Asset Owner can properly consider and additional actions which may be necessary.**

Having considered this DPIA, I see no high risks to the rights and freedoms of individuals which have not been adequately mitigated. Processing may therefore continue including in my view the additional collection of stills images where linked to reads in scope of this DPIA.

Sign Below:

Name: Darren Curtis Position: Data Office Date: 15.11.2021

Reviewed by Catherine Carrington 28/03/2020, 26/08/2020, 6/09/2020 and 16/12/2020.
This is now ready for Sign Off on 16/12/2020.

Distribution list

Recipient	Title	Location



Change control

Version	Date	Authority	Evidence of approval	Record of change



Appendix A – Glossary

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 2018	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 2018	HRA	Includes all subordinate legislation made under the HRA from time to time
Information		Any information however held and includes Personal and Special Category 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)
Pseudonymous		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
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
Personal Data		Personal data is information relating to a living identified or identifiable individual
Special Category Data		Special category data is information relating to racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life / orientation, criminal convictions and offences, related security measures or appropriate safeguards.



Appendix B – Document Handling Instructions

<p>To maintain the secure handling of this document, the below Handling Instructions MUST be read and complied with as part of your responsibilities in receiving this document. These instructions replace all other previous instructions which may have formed part of this document</p>	
<p>Authority for Publication</p>	<p>This document can only be made public on the explicit Authority of either or a combination of the following Authorities:</p> <ol style="list-style-type: none"> <u>During the lifetime of this Project</u> – the assigned Project Lead / Senior Information Risk Owner (SIRO)/ or the MPS' Data Protection Officer [or their nominated Deputy].
<p>Information Security [Access Controls] And Personnel Security Clearance [Vetting] [MPS Vetting Policy takes precedence]</p>	<p>.As well as those roles identified within the Front Cover of this document, this document can be made available to MPS staff involved with the MPS Gangs Matrix:</p> <ol style="list-style-type: none"> <u>For MPS personnel</u> - MPS Recruit Vetting (RV) or Counter-Terrorist Check (CTC) <p>Additionally, access is also reliant on a <u>direct need to know</u> basis.</p>
<p>Physical Security [Storage/offsite use of information] [Remote Working – Working Away From the Office - WAFTO]</p>	<p>This relates mainly to where there is a requirement to have access to this document away from an approved location [e.g. Working Away From the Office/ Homeworking, etc.].</p> <p>As such, where approval has been received [i.e. as part of your organisation's WAFTO policy, etc.], the following rules are to be applied:</p> <ol style="list-style-type: none"> Electronic access to this document remotely can only be from nominated locations and via appropriately accredited solutions, or stored on appropriately accredited devices (e.g. approved laptops, not your own device, etc.). Always be mindful of your surroundings and who else is within the vicinity their clearance/ 'need to know' When handling paper versions of this document away from the office, always be mindful of your surroundings. The document Must Not be reviewed when within public areas where there is a risk of 'shoulder surfing, lost/ theft, etc. (i.e. whilst on/within public transport, cafes, lobby areas, etc.). Always ensure that all paper versions are stored within a physically robust cabinet/ safe which also has a robust locking mechanism with access restricted to only authorised individuals.
<p>Electronic Security [Removable Media]</p>	<p>The document can be held/ processed Only on MPS corporately owned infrastructure/ issued devices [laptops, tablets]/ media [USBs, CDs, DVDs] or other ICT solutions, which have been approved by the MPS security personnel.</p>



To maintain the secure handling of this document, the below Handling Instructions **MUST** be read and complied with as part of your responsibilities in receiving this document. These instructions replace all other previous instructions which may have formed part of this document

<p>Movement [internal dispatch/ UK use of Post/ Courier Services]</p>	<p>The following despatched guidance/ instructions apply. <u>Where this document has a GSC marking of OFFICIAL</u></p> <ul style="list-style-type: none"> • Through the use of the MPS’ Internal despatch service – sealed envelopes/ containers with GSC marking and any other descriptors shown. • By trusted hand - in that it must be somebody with a security clearance appropriate for unsupervised access. The bearer of the document should (in theory) be able to access and read the document unsupervised. • For sending personal data outside the UK you must comply with Data Protection Act 2018. Initially seek advice from the Information Rights Unit (IRU) via an email to DPA Mailbox - SAR.
<p>Movement [Use of Post/ Courier Services outside UK] This also includes the use of Fax machines</p>	<p>The document Must Not be sent outside of the UK without first initially consulting with the Author for approval or the roles identified within the above Authority to Publication section of these Handling Instructions</p>



Appendix C - Operational Rationale for MPS Access to TfL ANPR data and imagery

Overview

The purpose of this report is to articulate the way in which the MPS would utilise TfL ANPR data and imagery should it be available for use in the total War on Crime. It is structured around current NPCC ANPR strategy, but elaborates on how it applies to or within the Metropolitan Police Service, and makes specific comment where there is 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 the police use of ANPR is to target criminals and terrorists and identifying those committing counter reconnaissance 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 police objective 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 and imagery. This is based on a rebuttable presumption that, where the value of ANPR data in pursuing the 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 NPCC values and applies then in respect of all its ANPR activity, including that already undertaken use TfL ANPR data and imagery 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 Act.



While a Vehicle Registration Mark (VRM) alone does not identify a particular individual, ANPR data will be treated as 'personal data'

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 recognizing 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 purposes.

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

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

ⁱ These statistics are readily available to the public on <https://www.met.police.uk/sd/stats-and-data/met/crime-data-dashboard/>