TFL ANPR: SHARING DATA AND IMAGERY WITH THE MPS

METROPOLITAN POLICE

Classification	Official
Suitable for Publication	Yes
Title	DPIA relating to the re-integration of TfL data feeds into the MPS ANPR system following the 2021 camera upgrade.
Purpose	To consider any privacy issues and mitigate any risks arising
Summary	TfL have updated their ANPR camera infrastructure. This required a reconfiguration of the network connections with the MPS ANPR system. TfL Cameras now must provide imagery as well as metadata, which requires consideration of further privacy implications. This DPIA assesses the impact of reintegration of the data feeds and the privacy impact on All road users of the enhanced data being accessed after a three year absence. The report concludes that the provision of access to the data is proportionate and necessary measure to maintain the safety and security of the capital.
Author	[redacted]
Version	28/01/25
Creating Unit	ANPR Unit -MO2 (Met Intelligence)
Date Created	19/10/2021
Review Date	Date reviewed 10/05/2023, 11/10/2023, 03/05/24, 28/05/24 and 26/07/24 and 24/09/24, 01/10/24, 04/10/24 and 15/10/24, 24/01/25 and 28/01/25
CYC Ref	01/DPA/23/004643 (Original DPIA 01/DPA/20/000569)

Contents

Appendices

METROPOLITAN POLICE

1. Privacy Impact Screening Questions

		Yes	No
Q.1	Systematic and extensive profiling or automated decision-making to make significant decisions about people.	☑	☐
	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.		
Q.2	Large-scale use of special category data or criminal offence data.	☑	☐
	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.		
Q.3	Systematically monitoring or profiling on a large scale, or in a public place.	☑	☐
	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.		
Q.4	Using new technology, or novel use of existing technologies.	☑	
	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.		
Q.5	Processing biometric or genetic data.	☐	☑
	This includes doing anything with DNA samples, DNA profiles and fingerprints.		
Q.6	Combine, compare or match data from multiple sources.	☑	☐

		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.		
Q.7		Process personal data in a way which involves tracking individuals' online or offline location or behaviour.	☑	☐

	This would not extend to individual targeted surveillance authorisations.	☐	☐
Q.8	Process personal data, which could result in a risk of physical harm in the event of a security breach.	☑	☐
	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.		

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 the camera network was upgraded in 2021.

The 2021 upgrade to TfL ANPR cameras affected over 700 sites around London. Technical challenges and governance issues stemming from this upgrade led to the MPS losing direct access to nearly all TfL cameras.

Regaining the connection to the enhanced TfL network would now mean that the MPS would also receive still images of the vehicle associated with the alpha-numerical number plate reading alongside the camera meta data (ie date. time, location). This is standard in modern ANPR cameras and is imagery is widely used to corroborate the ANPR data.

The MPS has worked with TfL to re-configure its connection to the TfL camera infrastructure with a view to regaining access to reads from all TfL ANPR cameras.

[redacted] cameras from the network were reintegrated on an exceptional basis to ensure public safety during the repatriation of HM the Queen and the royal funeral, and during the coronation of the King. Outside of these periods the MPS has not had access to TfL data feeds (except to a limited number of Monitoring Cameras).

Upgraded TFL Camera network

The MPS are currently able to reconfigure its connection to the TfL ANPR network to access the enhanced data, including imagery that is provided by the TfL cameras. This would also ensure that the MPS could access the previously accessible TfL Congestion Charging (CC), Low Emission Zone (LEZ) and Monitoring Cameras (Subject to availability). Please note the following:

- There is no immediate plan to request access to any additional cameras that were added to the TfL camera network as part of the 2021 upgrade or to enable the expansion of the Ultra Low Emission Zone (ULEZ) in 2023. This document will not consider the privacy impact of taking reads from any additional sites [redacted] – so access would only be regained to TfL ANPR cameras in the Congestion Charging zone and at sites originally used only for enforcement of the LEZ (predominately on the boundary of that Zone). These are cameras to which access was granted in 2015.

- 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, as well as be subject to the requirements of Mayoral Decision 2977.

- Privacy and equality impacts will be reassessed as key elements of any such process.

2. Benefits to the MPS, the public and other parties

Enhancing the accuracy and evidential value of the MPS ANPR system

In 2015 the MPS began taking reads directly from all TfL ANPR cameras then available. This access was confined to the ANPR data alone, without the accompanying visual imagery, [redacted]. This prevented 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. It should be noted that the ICO recognises that in order to comply with article 5 of the UK GDPR 7 principles, the inclusion of imagery alongside ANPR data enables operators of the system to ensure accuracy of the data.

The 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. The risk of collateral intrusion from the processing of imagery, and the privacy implications for specific communities and groups, is fully considered in an MPS Equality Impact Assessment, which has also been submitted to TfL.

Retention of access to the previously held TFL ANPR reads

Until the TfL upgrade programme, the MPS received around 8-10 million ANPR reads for the London area. 6-8 million of those came from the TfL system. This therefore made 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.

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 9 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, [redacted]

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.

The likelihood of achieving operational results with ANPR are, to a large extent, a function of the scale of the ANPR camera network. The more cameras a vehicle hits, the more opportunity there is to link it to a crime, layer ANPR data with other data sources, identify directions of travel, and to implement successful interventions.

The loss of the TfL data from the MPS ANPR system represented a reduction in the wider MPS ANPR capability. [redacted]

[redacted]

It is also important to note that the TfL ANPR cameras are disproportionately concentrated in central London [redacted]. The area cover also contains [redacted]

Efficient and cost effective maintenance of the MPS ANPR infrastructure

Much of the MPS' own 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 behaviour 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.

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.

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 Biometrics and Surveillance Camera Commissioner's requirements for justifying new ANPR infrastructure.

Any future proposal to take reads from additional TfL cameras, such as those deployed in the 2021 TfL camera expansion, will be treated in the same way as new MPS infrastructure and reviewed through a process which is compliant with these requirements, and with MD 2977. A case setting out the operational proportionality and necessity would 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), prior to submission to TfL. Where the case is made out and reads taken, this DPIA and the parallel Equality 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 regaining access to TfL ANPR data and to increase the accuracy of the ANPR dataset by adding corroborating visual imagery.

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

TfL own and maintain Congestion Charge, LEZ Enforcement and Traffic Monitoring cameras. All of the TfL cameras at sites in existence prior to the 2021 camera expansion fed data into the MPS ANPR system – comprising of over 700 sites.

Previously the MPS only received the textual data, (VRM, Date, time, location) from the TfL data feed. The camera upgrade in 2021 required compatibility work to ensure that, if authority was granted, connections to the MPS system could be made to 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 also assists 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.

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

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

The National ANPR Standards for Policing and Law Enforcement (NASPLE) Technical specifications, places significant restrictions to limit image size, (Just 3KB or 120 x 60 pixels for plate patches or just 25kb for overview images) 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 MPS ANPR system is automatically downgraded to ensure compliance.

The MPS has a written equality impact assessment in place that considers the issues and potential risks associated with the establishment of an individual's race and or gender which should be referenced for further detail.

The MPS only use ANPR data in the furtherance of police business, comprising activities that are consistent with a lawful policing purpose. 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.

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

All TfL ANPR data (including the accompanying visual imagery) that is shared with the MPS will be stored (in compliance with NASPLE) within the MPS ANPR system. This 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 MPS ANPR system 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 MPS ANPR system. This facility is subject to all the same .deletion protocols as the MPS ANPR system however the user group is restricted to only 4 fully trained and qualified individuals within the ANPR Technical Support Team.

The MPS ANPR system 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 MPS ANPR system. 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. See the following link for more information on the Management of Police information, and the College of

police guidance on this subject. https://www.college.police.uk/app/information-management/management-police-information

Each request for storage beyond 12 months in the evidence locker is made in accordance with MOPI guidance according to crime type.

Data relating to every case held in the evidence locker is reviewed by the MPS Audit team in line with the national NASPLE guidance for auditing. Records are checked every 6 months to verify whether the data retained is still required, and that it still meets the requirements for retention. The officer in charge, or the requesting officer, is contacted to verify whether the data is still required for evidential purposes. As of May 2023 if nothing is heard in response to this request an escalation will be made to their supervisors. If nothing is heard after three attempts, or if the OIC or requesting officer confirms that the data is no longer required, the data in the evidence locker will be deleted from the system by the Audit team.

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

Access to MPS ANPR system 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, that the 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 or 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 'Managing Police Information' and its predecessor '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 MPS ANPR system 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.

There is a tight process around how VRMS are added to the VOI and Violence Suppression Hotlist (VSH.) This is in part determined by the published National Police Chief Council Regulation 109 document[1], which details requirements for the intelligence used to create VOI lists and PNC markers

There is an expectation that all officers in the MPS flag intelligence reports as "ANPR noteworthy" when a vehicle is involved. The Met Intel ANPR team will them add these vehicles to the most appropriate list, [redacted]

Note that the referrals are generated by, and focused on, the VRM. Descriptions of known owners and drivers may be added to the entry, but they are not relevant to the VRM being added to a list.

The decision [redacted] is determined by reference to suspected criminal activity and intelligence, regardless of personal characteristics. As such, any disproportionality is reflective of disproportionalities in wider criminal demographics, not with disproportionalities created by ANPR.

Note that the Met Police EQIA relating to Violent Harm Assessments (published January 2024) has noted the disproportionalities in individuals involved in violent crime: police data indicates that young, black men are disproportionally represented as offenders of crime and serious violence, and the VOI lists and VSH. Around 65% of individuals on the MPS VHA are non-white. This includes 58% of suspects for knife-related assaults, 54% of suspects for Lethal Barrelled firearms offences and 65% of suspects for robbery (data from MPS figures, 2023)

All requests for usage must be made through a tasking process, and only serious crimes will routinely be deemed suitable for ANPR. Any usage of ANPR that could entail surveillance must be backed by a Directed Surveillance Authority (DSA) under the Regulation of Regulatory Powers Act 2000 (RIPA), and signed off by a senior officer.

The quality of the imagery provided by ANPR cameras is purposely throttled down to ensure that it cannot routinely provide images inside vehicles, and thereby is recognised as not being "intrusive" in the legal sense related to surveillance. This is fully detailed in the Home Office guidance on technical standards

[1] https://assets.publishing.service.gov.uk/media/64ac1bddb504f70012cdb88a/Reg_109_Supplier_Specification_V2.4_FINAL.pdf

and audit (see above links.)

As with any system in any organisation using privileged data, there is always the danger of insider threat or misuse. Any misuse of police ANPR systems by MPS employees or officers would be likely to constitute a criminal offences, as well as encountering disciplinary processes, much in the same way misuse of intelligence systems.

Note that full access to ANPR tools is granted only to specialists with enhanced vetting. Moreover, all users are subject to randomised auditing by a separate ring-fenced unit.

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

All ANPR data which includes electronic imagery is held in the MPS ANPR system, 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 and imagery based on permissions which limit access up to 90 days or up to 12 months of data. Data and imagery is deleted permanently as per Home Office NASPLE guidelines. This deletion process is an electronic and manual deletion of data/imagery. A residual risk remains of electronic software being used to recover deleted data/imagery 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/imagery 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 privacy 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/imagery are responsible for deleting data and associated images 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 and images are only retained for 12 months. An automated process is currently in place to ensure the system automatically removes data and images once it has reached the 12 months retention period. Data and images 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 and associated images.

The MPS ANPR system 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 (MPS ANPR system), however the data is owned and managed by the MPS.

The MPS ANPR unit will generally average [redacted] on VOI hotlists on any given day, together with around [redacted] on the Violence Suppression Hotlist. The limited numbers highlight the fact that that the use of hotlists/ VOI lists is carefully curated. Note also that there are strict processes to remove vehicles from the lists. Reviews take place on every listed vehicle after 14 days. They only remain on the lists if there is continued belief that they are involved in criminality.

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.

Article 10: Freedom of expression

3. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
4. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 11: Freedom of assembly and association

5. Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.

6. No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, 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. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.

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).

The use of ANPR provides a means of monitoring the movements of a vehicle, and from that law enforcement bodies can gain a means of building a "life-styling" picture. Law enforcement uses ANPR explicitly for this purpose to fight crime. However, the MPS use of ANPR in this regard is governed by legislation and policy, particularly NASPLE and the associated technical and audit specifications on ANPR usage. All ANPR usage must also pay regard to RIPA, which sets clear parameters for intrusion, not least in the requirement to have a Directed Surveillance Authority in place for any usage of the data that would provide invasive (in the general meaning of the word) monitoring of an individual's movements.

The MPS in considering how the deployment of ANPR technologies in public places recognises that there may be a potential interference with an individual's Art 10 European Convention on Human Rights ("ECHR") right of expression, which may for example be manifested in the form of public protest; and the art 11 ECHR right of assembly. Protests for example may express lawful opinions which are not necessary consistent with the position of the state on the same topic and given the power of the state over citizens and individual may feel vulnerable should their identity be captured at an individual level, rather than through the relative anonymity of a group. ANPR cameras are static at a point and record vehicles passing a point. Albeit that some cameras are deployable to respond to need, they are designed and deployed to capture and process number plates. In some cases number plates may be resolved back to an individual through the exercise of additional police investigative measures by virtue of combination with other information. In this respect, ANPR is much less intrusive than other forms of surveillance because it is, above all, a tool for establishing the location of a vehicle in a particular location at a particular point in time. The police must take additional investigative steps to (a) establish who the registered keeper is, which may be a company rather than an individual, and (b) who was actually driving the vehicle at that moment in time as many vehicles are used by people other than the registered keeper.

Given that the registered keeper may not be the individual who drove the vehicle, at the time their Art 8 right to privacy would be engaged to the extent that the police may need to take steps to eliminate them as the driver (or passenger) of a vehicle. Articles 8, 10 and 11 of the HRA are qualified rights and in the context of preventing crime and investigating criminality etc., the limited intrusion described is necessary in a democratic society for those purposes and for the wider benefit of all society. The MPS position is therefore that such interference is lawful, necessary and proportionate to meet a legitimate aim. This is because police frequently have to eliminate individuals as suspects, which may include identifying a registered keeper of a vehicle so that a suspect can be identified.

The capture of a vehicle number plate by ANPR cameras is less intrusive than the video imagery captured by the CCTV cameras which are common place across London in public and private settings. Unlike most CCTV, ANPR does not capture moving imagery, and it is not intended to capture facial imagery. ANPR is categorically focussed on the momentary capture of a number plate. The quality of the imagery provided by ANPR cameras is purposely throttled down to ensure that it cannot routinely provide images inside vehicles, and thereby is recognised as not being "intrusive" in the legal sense related to surveillance. This is fully detailed in the Home Office guidance on technical standards and audit. ANPR is not designed specifically to capture moving images to the level sufficient for human identification, nor does it include audio (both dimensions of which would engage a higher level of intrusion than is

actually the case). Where ANPR captures a number plate, the keeper is not necessarily the owner or driver, and, as such, police will always be reliant on other information to attribute a VRM to an individual. This limits the intrusion.

Where intelligence or evidence indicates that it is necessary and proportionate to understand the movement of a vehicle, before or after an event, then they may be added to the watch list, or an interrogation may take place to establish whether within the preceding 90 days the passage of the vehicle passed a camera has been recorded. In cases of serious crime (as defined in the NASPLE policy) checks can be made over the preceding year.

It could be argued that someone fearing that they might be subject to having their number plate and therefore potentially their location (subject to them being the driver or a passenger at the time) captured at a particular time may be less likely to exercise their article 10/11 HRA rights. However, the MPS notes that the vast majority of subjects who wish to attend protests do so using public transport and would remain unaffected by the use of ANPR within the TFL area.

The MPS adheres to policy and guidance which ensure that the use of ANPR is limited to serious crime, the protection of national security, public safety and the prevent disorder or serious crime. It is only used when proportionate and necessary in these areas. The guidelines for the use of ANPR are clearly stated in the published policy and guidance, in particular NASPLE and the related technical and audit standards.

All reactive requests for ANPR data must be made through a tasking process, and only serious crimes – as defined in the published NASPLE guidance - will routinely be deemed suitable for ANPR. The use of ANPR for "volume" crime needs to be authorised by an Inspector with a rationale – such as heightened community concerns. Any usage of ANPR that could entail surveillance must be backed by a Directed Surveillance Authority (DSA) under the Regulation of Regulatory Powers Act 2000 (RIPA), and signed off by a senior officer.

There is a tight process around how VRMS are added to the Vehicle of Interest lists, and the Violence Suppression Hotlist (VSH.) This is in part determined by the published National Police Chief Council Regulation 109 document, which details requirements for the intelligence used to create VOI lists and PNC markers

There are rigorous safeguards around the generation and processing of intelligence that leads to inclusion on hotlists and Vehicle of Interest lists. This includes strict guidance on the weeding of information that is at risk of being out of date. Any vehicles on Vehicle of Interest (VOI) lists will be added following criminal intelligence, and a proportionality and necessity test.

There is an expectation that all officers in the MPS flag intelligence reports as "ANPR noteworthy" when a vehicle is involved. The Met Intel ANPR team will them add these vehicles to the most appropriate list, [redacted]

Note that the referrals are generated by, and focused on, the VRM. Descriptions of known owners and drivers may be added to the entry, but they are not relevant to the VRM being added

	to a list. ***The decision to place individuals on hotlists is determined by reference to suspected criminal activity and intelligence, regardless of personal characteristics.*** ***Finally, it should be noted that ANPR data usage in law enforcement would only impinge in these protected areas within constraints stated in policy, such as NASPLE, in related legislation, such as RIPA, and in associated codes of practice.*** ***The MPS acknowledges that there is disproportionality within the individuals linked to vehicles within the Vehicles of Interest List and named within Violence Suppression Hotlist. The MPS monitors disproportionality actively to ensure that where it exists, the causes are understood and can be rationally explained and justified. Should any unjustified disproportionality ever be identified, appropriate measures are implemented to remediate the balance. The current situation may be explained as follows: In the case of the nature of offending which ANPR is necessarily being deployed against, intelligence and evidence demonstrates disproportionate representation. As highlighted below for example, at the time of the analysis 65% of suspects for robbery were non-white. We are confident that this bias is not caused by discrimination.*** ***The decision to place individuals on hotlists is determined by reference to suspected criminal activity and intelligence, regardless of personal characteristics. As such, any disproportionality is reflective of disproportionalities in wider criminal demographics, not with disproportionalities created by ANPR.*** ***Note that the Met Police EQIA relating to Violent Harm Assessments (published January 2024) has noted the disproportionalities in individuals involved in violent crime: police data indicates that young, black men are disproportionally represented as offenders of crime and serious violence, and the VOI lists and VSH. Around 65% of individuals on the MPS VHA are non-white. This includes 58% of suspects for knife-related assaults, 54% of suspects for Lethal Barrelled firearms offences and 65% of suspects for robbery (data from MPS figures, 2023)***
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 Practise 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 August 2023 and August 2024 approximately 1 million crimes were reported to the MPS. Around half these were violence related with further incidences showing high proportions of theft, burglary and vehicle crime. [2]

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 2022-2025 London's Police and Crime Plan 2022-25 | London City Hall , 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 by vehicle 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, often by vehicle.

Serious Youth Violence – Often involving rival groups whose focus is territorial. Will involve perpetrators travelling by vehicle to commit offences. Reducing 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.

[2] https://public.tableau.com/app/profile/metropolitan.police.service/viz/MonthlyCrimeDataNewCats/Coversheet

Trafficking, Child Exploitation and Modern Slavery – Involves a victim being moved, often by vehicle, 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 by vehicle 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 by vehicle across policing boundaries to commit offences.
Firearms/ Drugs/ Money – Often moved by vehicle 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.

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 behaviours 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 by vehicle.

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 in 2020. 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 in 2021 to support the MPS' aim of supressing 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.

Regaining access to TfL ANPR data is imperative for the MPS in continuing to protect Londoners. The addition of imagery 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 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.

The risk of collateral intrusion from the processing of imagery, and the privacy implications for specific communities and groups, is fully considered in an MPS Equality Impact Assessment, which has also been submitted to TfL.

[redacted]

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 who use the road network. As already stated above the drivers of London are captured 8-10 million times per day on MPS and TfL ANPR systems. The TfL cameras previously fed 6-8 million reads into the MPS systems. 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.

The loss of the TfL ANPR reads has compromised the ability of the police to tackle some high-harm criminality in areas such as modern slavery, violence against women and girls, county lines offending, gang violence, and all other types of organised criminality. The loss of these camera feeds has also compromised the ability of the MPS to fulfil safeguarding obligations, such as the location and interception of people with serious mental health issues. The loss of the camera feeds [redacted] Finally, the loss of these cameras has forced to the MPS to constantly flex its own small stock of cameras to service urgent needs, placing huge cost and resource demands on an overstretched public organisation, and creating regular difficult opportunity-cost calculations on how best to protect the public.

The wide and integrated nature of the ANPR camera network in London is critical to delivering on these vital policing commitments. Complex ANPR enquires rarely rely on a single camera feed - data points are almost invariably required from a number of locations. As such, it would be fundamentally impracticable to request data directly from TfL on an ad hoc basis. In fast moving situations the MPS relies on instant updates to track vehicles as they move – seconds can be vital and it would be operationally impossible to make requests, 247, in such circumstances. Moreover, in fast-moving situations policing relies on [redacted]. With regard to retrospective enquires, TfL can only store ANPR data for a limited period (fewer than 30 days, unless a Penalty Charge Notice is issued or payment is made using an AutoPay account). National guidance permits policing to store ANPR data for 12 months – a facility that is vital in the MPS's ability to investigate crime, not least as police may not be aware of the need to acquire particular data until weeks have past. Also, when completing complex multi-source layered enquires, investigators will only see the connections between data if it is part of the integrated data platform – officers will not be able to make ad hoc data requests for data they don't know is there. For these reasons it is vital that the TfL data feeds directly into the MPS systems.

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 publically available material such as the MPS website and the MPS ANPR survey undertaken in 2021. Although the exact locations of the cameras are 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. In order to be able to investigate current and historic crimes the entire ANPR data set is required as any one of the the VRM's held could be critical to a criminal investigation. Without all the data being available it would be impossible to fully investigate crimes. Through the guidance in NASPLE it ensures all policing systems only hold this data for a 12 month period, providing time for emerging and historic investigations to take place while achieving data minimisation.

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, compared to the situation before the TfL camera upgrade in 2021. The inclusion of heavily restricted imagery will only enhance its accuracy and will not provide significantly more private information. There are no immediate plans to take data from the additional cameras added by TfL in 2021 and 2023, 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, prior to submission to TfL.

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 and movements of a vehicle. Any other form of digital intelligence capture e.g. 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. 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.

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 previous capability it is reasonable to extrapolate that this is equally proportionate and necessary.

Clearly the use of the 2021 expanded TfL camera 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 risk of collateral intrusion from the processing of imagery, and the privacy implications for specific communities and groups, is fully considered in an MPS Equalities Impact Assessment, which has also been submitted to TfL.

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 Independent advisory groups IAG'S, and to feed back any significant community sentiments. If strong feelings are identified, Community Impact Assessments and outreach work will be considered. Whilst this work is ongoing, the MPS has yet to see any significant issues raised from public consultation.

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.

If there is a legal requirement to process the information
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:
Protecting life and property
Preserving order
Preventing and detecting offences
Bringing offenders to justice
Any duty or responsibility of the police arising from common or statue 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:

METROPOLITAN POLICE

- **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 | Metropolitan Police 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 TfL documents are openly available on line.

TfL also publishes a privacy notice in relation to its own use of ANPR cameras for road user charging purposes. This also includes a section on camera sharing with the MPS

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.

METROPOLITAN POLICE

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. Retention of all ANPR reads for a 12 month period is required to ensure that emerging criminal investigations can be supported as well as investigations into crimes committed in the past. It has been argued that the data could be retained for a longer period to assist in the investigation of crimes where the investigation or the crime is reported years later. However this was assessed by the National Police Chiefs Council in conjunction with the ICO in 2017 and it was deemed proportionate and necessary to limit the retention period to 12 Months. This provided sufficient time for most crimes to be investigated and limited the impact to subject rights.

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.

The inclusion of imagery in the reintroduced data feed supports other data protection principles such as ensuring that data is accurate.

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 of 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.

METROPOLITAN POLICE

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 produced by the Home Office, the owner of the NAS .

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

Any personal data (with the exception of associated images which are of too low quality) 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 (to NASPLE standards to 98%) of what has been captured. Vehicle imagery will enhance the ability to confirm the accuracy of the data gathered.

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:

Retention and deletion policy

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 and associated images can be saved in the MPS ANPR system "Evidence Locker" and retained under MOPI guidelines. Data and images 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. The necessity for Data and images subject to retention under MOPI is regularly reviewed, and governed by MOPI guidelines https://www.college.police.uk/app/information-management/management-police-information

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 number plate images (and associated photographic imagery) will be deleted from MPS ANPR system 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 implement a range of security measures to protect this data from external attacks in line with the National Cyber Security Centre guidance.

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

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 i.e. number plate images. The National ANPR Standards for Policing and Law Enforcement (NASPLE) Technical specifications, places significant restrictions to limit image size, (Just 3KB or 120 x 60 pixels for plate patches or just 25kb for overview images) 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 restrictions are a pragmatic approach to the probable bandwidth processing and storage requirements that HD imagery would require. The ANPR cameras are set up by TfL and only capture the imagery required by TfL for road user charging purposes. Overview images are typically zoomed out and are insufficient for identifying anything beyond make, model, VRM and colour of passing vehicles 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.

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 2021 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

METROPOLITAN POLICE

- 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.

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. To exercise any of these rights please contact the Information Rights Unit at: mpsdataoffice@met.police.uk.
2.	Transfers Outside the European Union (EU)
	UK GDPR Recital 44 *(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

METROPOLITAN POLICE

4. Consultation Results

	Date	Method of Consultation	Stakeholder	Outcomes
1	June - July 2021	Canvass of over 2500 London residents.	MPS	A number of key extracts are shown below in the annex, together with the provided demographic data of the participants. The survey showed overwhelmingly high levels of support for the MPS using ANPR to fight crime and to keep the public safe. There was a high level of support shown for working with partners, such as TfL. 80% of respondents, for example, replied that they would support increased deployment of ANPR in their area. 80% also responded that TFL sharing ANPR data with the MPS helps make London safer.
2	June 2023	Strategic Community Impact Assessment	MPS	A Pan-London Community Impact Assessment was completed in June 2023 by the MPS Strategic Engagement Team (SET) in order to assess attitudes towards to upgrade in all significant religious, national and racial communities in London. There has been a standing agreement for some time that any emerging tensions around ANPR would be brought to the attention of MO2 by SET. This will be updated on an annual basis.

3	28th May 2020	ANPR IAG meeting – Chaired by the Surveillance Camera Commissioner (SCC) (Now known as the Biometrics and Surveillance Camera Commissioner)	Various – public, regulators, Government Bodies	Various recommendations to ensure that the taking of additional TfL data was based on proportionality and necessity rather than opportunity and cost. 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.
4	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.
5	04/06 – 23/07/2021	London Specific ANPR survey to cover sharing of data from TFL and wider ANPR use	Public	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 2021 camera expansion in the future. 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

				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 TFL camera network expansion.

4.	20/07/21	ANPR IAG – Chaired by SCC	Various – public, regulators, Government Bodies	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 TFL camera expansion was presented to the members who were largely appreciative of the change of approach. 2 concerns were raised by members of the group. **It was suggested that the MPS could still end up with a 'ring of steel' and therefore should assess / consult on that basis.** 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. **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.** This suggestion has been considered on a number of occasions. The Mayor / MOPAC are fully sighted and have given approval for the sharing of the TFL data.

				document and other governance measures. 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. 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.

5. Balanced Risk Assessment

	Risk	Likelihood L/M/H	Impact L/M/H	Solutions/ Mitigations	Residual Risk	MPS SIRO Sign-Off
	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	
	MPS data is leaked or accessed by those outside of the organisation.	L	H	The data is held within a secure data 'warehouse' and is accessed via the MPS ANPR system on Aware. Access is limited to specific Officers and appropriate cyber security measures are in place.	Medium	

	Data leaked by officers/staff who have access to the data	L	H	Appropriate audit processes are in place to limit access to ANPR 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.	Low	
	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	
	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	
	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. 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 regains access to data from TfL ANPR sites which previously fed into the MPS, and regains the operational effectiveness of its current ANPR capability.

The project will also allow the MPS to capture imagery alongside the textual ANPR data 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 2021 expanded TFL Camera 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 has shown high levels of support for police access to TfL data and images. There is no reason to believe that this support will diminish due to additional cameras being used on the network.

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.

METROPOLITAN POLICE

7. Data Protection Impact Assessment Sign-off

1. *Head of Information Law and Security*

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 regain the 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

METROPOLITAN POLICE

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 reeds in scope of this DPIA.

Review 05.05.2023

I have been asked to consider minor changes to the current DPIA as a result of the business' ongoing consultation with TFL. I take the view that whilst the document has been further enriched, no material change has taken place to the risks of processing. The key future risk remains the question as to whether the MPS should embrace the opportunity to harvest ANPR and related image data from the 2024 TFL expanded camera network. Should this step be considered important then appropriate contemporary consultation should take place and alongside a developed argument in respect of necessity and proportionality incorporated into a further DPIA review.

Having reviewed my previous observations/recommendations, progress has been made in ensuring that material stored in the evidence locker is retained in line with MoPI and subject to deletion when no longer required.

At this time, I see no high risks to the rights and freedoms of individuals which have not been adequately mitigated. Processing may therefore continue.

Review 01.08.2024

I have reviewed this DPIA which is once again revisited as a result of the ongoing consultation between the business and TFL regarding access to the camera network. I am satisfied that from a Data Protection Perspective, the business has adequately described the lawful basis and privacy implications for this processing, together with considering the

privacy interests of those that would potentially be intruded upon. Moreover, a case has been set out describing why in all of the circumstances and considering the controls and safeguards in place, that such processing from a MPS perspective is considered both necessary and proportionate. I note also that my observation regarding the potential for over retention in the evidence locker has now been addressed by way of more robust practice.

I am of the view that subject to the controls and ways of working set out herein that there are no residual high risk to the rights and freedoms of individuals that haven't been otherwise been mitigated. It therefore remains for TFL to choose to provide the access required given that subject to the approval of the Met's decision maker there appears to be no Met impediment to this processing commencing.

Darren Curtis 01.08.2024

Review 29.01.2025

I have reviewed this DPIA, which continues to evolve and address privacy issues as they arise. I not that in particular the author has highlighted how the MPS considers broader right beyond just that of privacy (Art 8 HRA) and has concluded that Art 10 and 11HRA may also potentially be interfered with where in particular someone might feel less inclined to assemble or protest if they believed that they may be subject to police monitoring through the use of ANPR. The MPS contends that as these are qualified rights, they may be fettered where such interference is necessary in a democratic society and that the interference is lawful and proportionate. The MPS recognises that interference with a qualified right is a significant step and therefore applies an authorisation process over the use of ANPR which I understand to be consistent with the published NASPLE policy.

The MPS monitors disproportionality in respect of those potentially affected by ANPR by virtue of inclusion of vehicles they are linked to being on ANPR monitored lists. Currently the MPS contends that the demographic distribution of persons affected is reflective of that which is demonstrated in the crime types of current interest and concludes that this is not driven by discrimination and can be lawfully justified. Monitoring allows for steps to be taken should any disproportionality be beyond proper explanation.

I am satisfied that from a Data Protection Perspective, the business has adequately described the lawful basis and privacy implications for this processing, together with considering the privacy interests of those that would potentially be intruded upon. Moreover, a case has been set out describing why in all of the circumstances and considering the controls and safeguards in place, that such processing from a MPS perspective is considered both necessary and proportionate.

I am of the view that subject to the controls and ways of working set out herein that there are no residual high risk to the rights and freedoms of individuals that haven't been otherwise been mitigated. It therefore remains for TFL to choose to provide the access required given that subject to the approval of the Met's decision maker there appears to be no Met impediment to this processing commencing.

Sign Below:

Name: Darren Curtis Position: DPO Date: 29.01.2025

2.	*Project Sponsor*
	I am the Senior Responsible Officer in the MPS for ANPR and have been close to this work with TFL since 2022. I have had significant conversations with TFL, ANPR teams, the Data Office and others to support this work. These TFL cameras are part of our overall approach to ANPR. Their addition to our network is, in my view, a necessary and proportionate step to help solve crime, protect the public and counter terrorism is London. There is a strong evidence base supporting the importance of ANPR and a clearly articulated impact assessment in relation to data protection and the protections on individual rights. ANPR does not directly identify a single individual, its use is regulated by national guidance. I am confident that in progressing this work, the MPS is taking appropriate steps to balance the need to fight crime and protect individual data rights. Signature: B A A Russell Name: Ben Russell Rank: Deputy Assistant Commissioner Date: 29/01/2025

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

ANNEX: Consultation Data

There have been a number of consultations held to gauge public attitudes towards the use of ANPR for law enforcement.

Two significant surveys into the use of ANPR for law enforcement were carried out in the Summer of 2021.

MPS Survey of June /July 2021

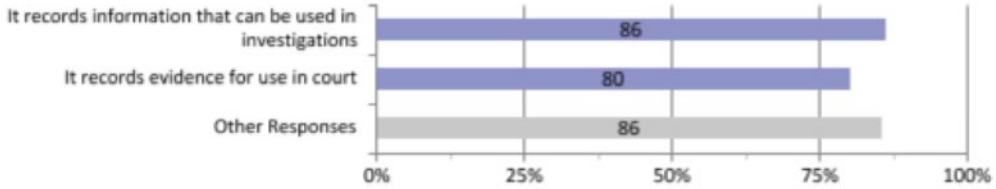
An MPS survey carried out in June/July 2021 canvassed over 2500 London residents. A number of key extracts are shown below, together with the provided demographic data of the participants. The survey showed overwhelmingly high levels of support for the MPS using ANPR to fight crime and to keep the public safe.

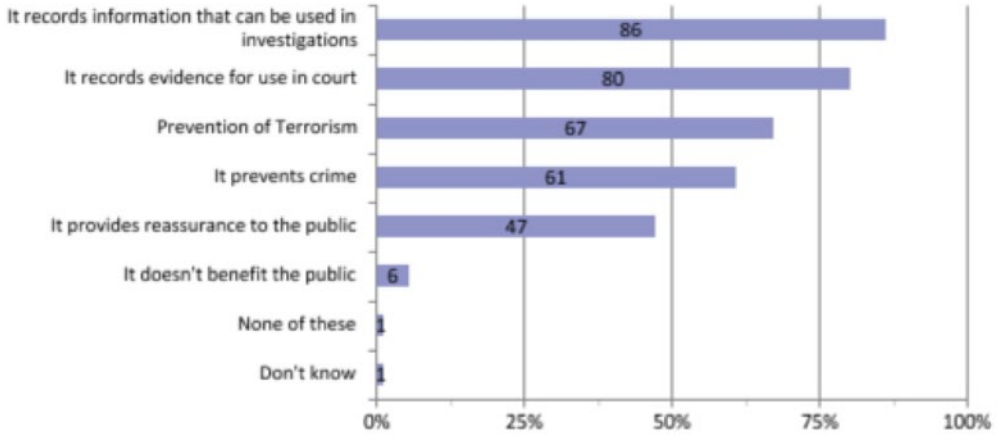
There was a high level of support shown for working with partners, such as TfL. 80% of respondents, for example, replied that they would support increased deployment of ANPR in their area. 80% also responded that TFL sharing ANPR data with the MPS helps make London safer.

A2 - *How do you think ANPR Camera usage benefits the wider community?*

It records information that can be used in investigations	86%
It records evidence for use in court	80%
Other responses	86%
Hide other responses	
Prevention of Terrorism	67%
It prevents crime	61%
It provides reassurance to the public	47%
It doesn't benefit the public	6%
None of these	1%
Don't know	1%

Base 2537 (Valid response 100%)
Confidence Interval 2% at 95% confidence

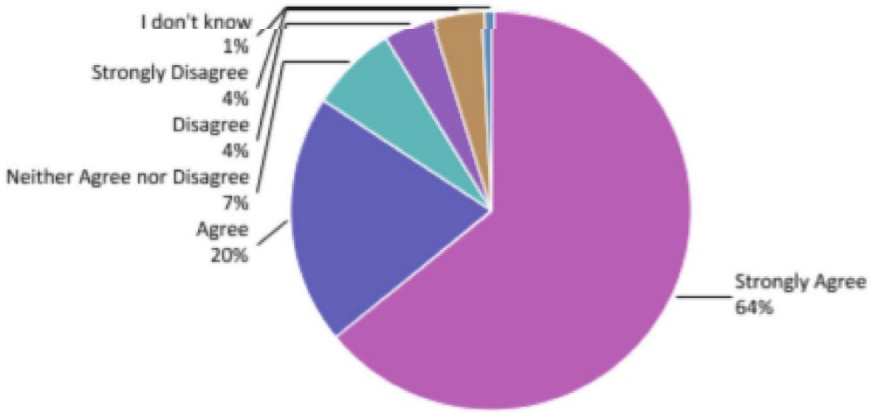




A3-1 - How strongly do you agree or disagree with the police use of ANPR cameras and data for the following purposes?...Generally by police forces and law enforcement agencies

Strongly Agree	64%
Agree	20%
Neither Agree nor Disagree	7%
Disagree	4%
Strongly Disagree	4%
I don't know	1%
Total	100%

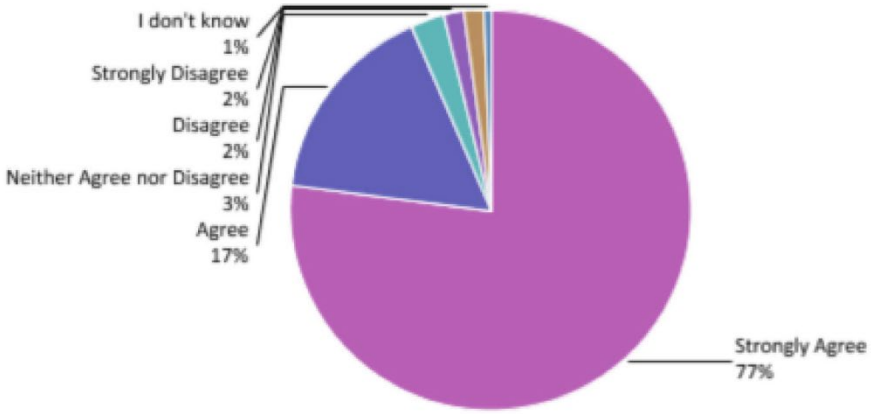
Base 2537 (Valid response 100%)
Confidence Interval 2% at 95% confidence



A3-2 - How strongly do you agree or disagree with the police use of ANPR cameras and data for the following purposes?...To deal with criminal behaviour

Strongly Agree	77%
Agree	17%
Neither Agree nor Disagree	3%
Disagree	2%
Strongly Disagree	2%
I don't know	1%
Total	100%

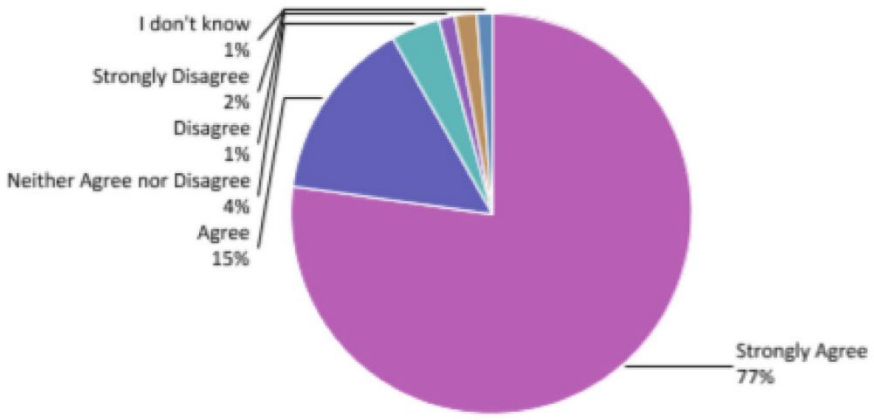
Base 2537 (Valid response 100%)
Confidence Interval 2% at 95% confidence



A3-4 - How strongly do you agree or disagree with the police use of ANPR cameras and data for the following purposes?...For counter terrorism purposes

Strongly Agree	77%
Agree	15%
Neither Agree nor Disagree	4%
Disagree	1%
Strongly Disagree	2%
I don't know	1%
Total	100%

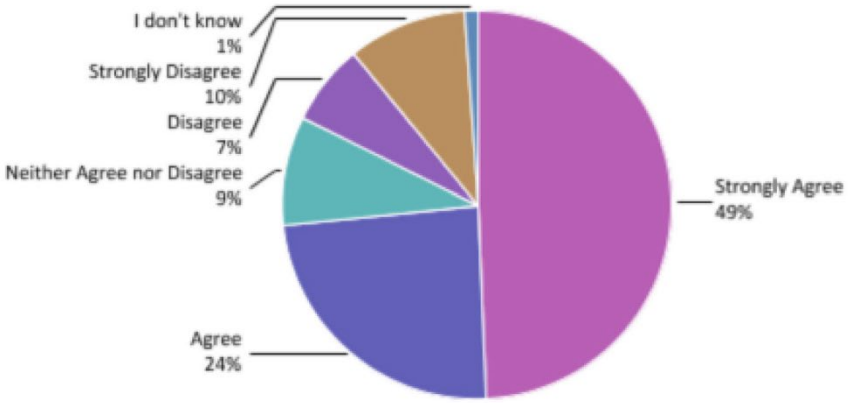
Base 2537 (Valid response 100%)
Confidence Interval 2% at 95% confidence



A4-1 - How strongly do you agree or disagree with the police use of ANPR cameras and data in the following circumstances?...In partnership with other agencies (e.g. accessing data from council owned cameras, Transport for London)

Strongly Agree	49%
Agree	24%
Neither Agree nor Disagree	9%
Disagree	7%
Strongly Disagree	10%
I don't know	1%
Total	100%

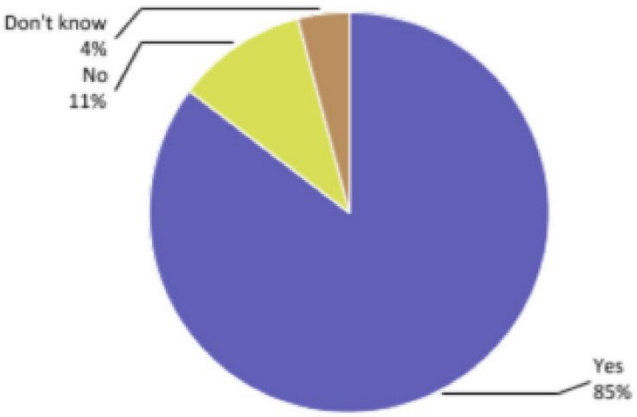
Base 2537 (Valid response 100%)
Confidence Interval 2% at 95% confidence



A8 - Do you understand why police forces and law enforcement agencies do not reveal the location of ANPR cameras?

Yes	85%
No	11%
Don't know	4%
Total	100%

Base 2537 (Valid response 100%)
Confidence Interval 1% at 95% confidence

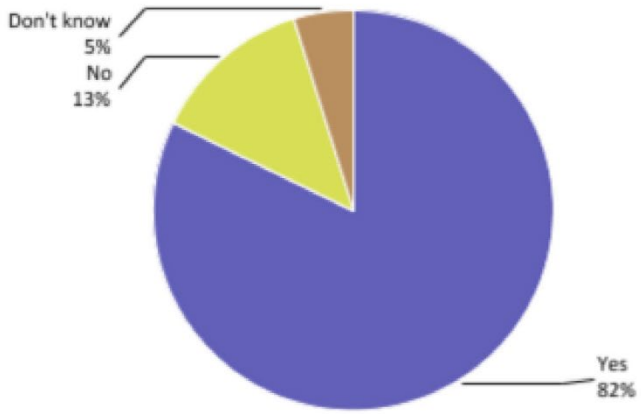


B3 - Would you support the increased deployment of ANPR cameras for policing purposes in your area?

Yes	82%
No	13%

Don't know	5%
Total	100%

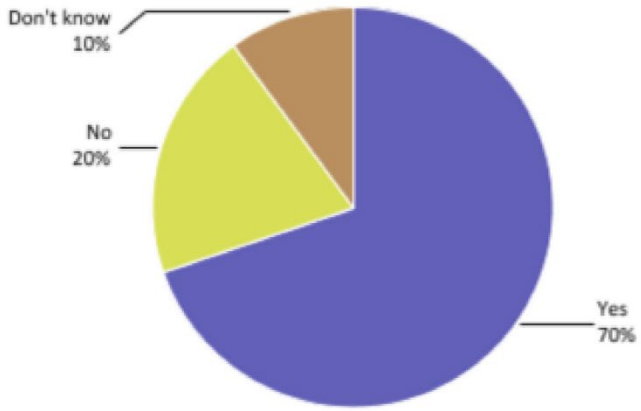
Base 2537 (Valid response 100%)
Confidence Interval 1% at 95% confidence



B5 - Do you believe that public organisations such as MPS, TfL and Councils etc should work together and share ANPR information to make them more effective and save money?

Yes	70%
No	20%
Don't know	10%
Total	100%

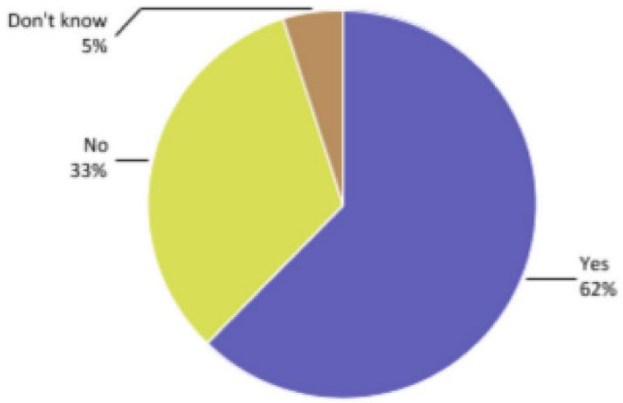
Base 2537 (Valid response 100%)
Confidence Interval 2% at 95% confidence



B6 - Did you know the MPS has access to TfL cameras for policing purposes?

Yes	62%
No	33%
Don't know	5%
Total	100%

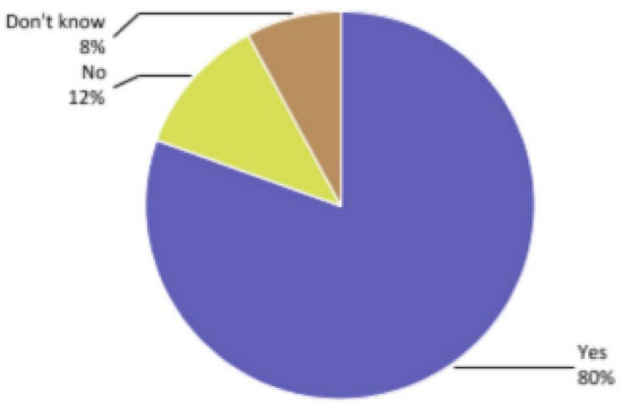
Base 2537 (Valid response 100%)
Confidence Interval 2% at 95% confidence



B7 - Do you believe that sharing TfL ANPR camera data with the MPS helps to make London safer?

Yes	80%
No	12%
Don't know	8%
Total	100%

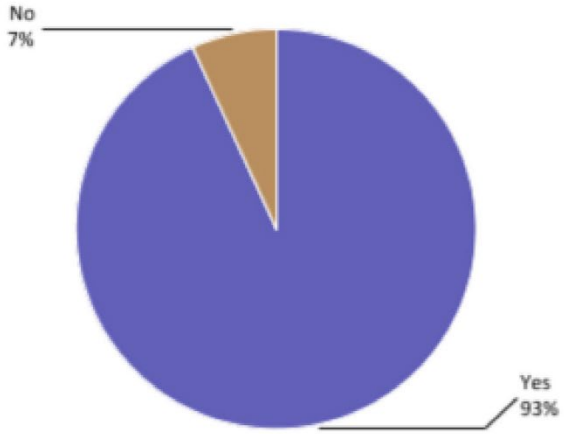
Base 2537 (Valid response 100%)
Confidence Interval 2% at 95% confidence



C1 - Do you use a vehicle?

Yes	93%
No	7%
Total	100%

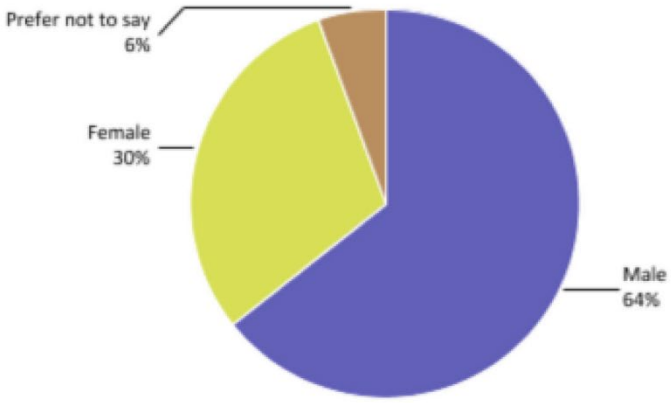
Base 2537 (Valid response 100%)
Confidence Interval 1.0% at 95% confidence



D1 - What is your gender?

Male	64%
Female	30%
Prefer not to say	6%
Total	100%

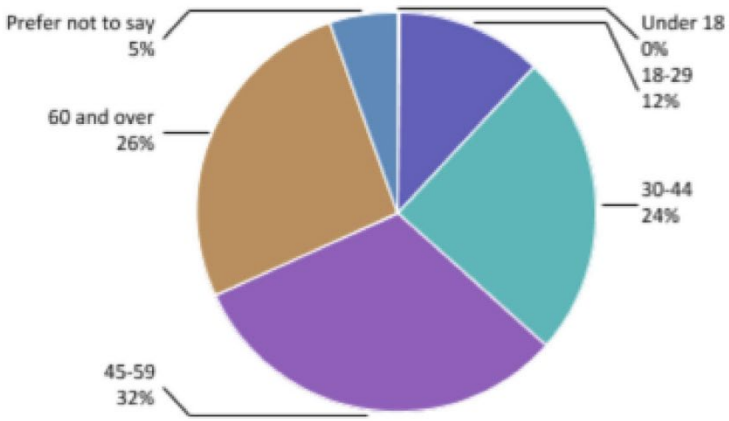
Base 2530, Not answered 7 (Valid response 100%)
Confidence Interval 2% at 95% confidence



D2 - What is your age?

Under 18	*%
18-29	12%
30-44	24%
45-59	32%
60 and over	26%
Prefer not to say	5%
Total	100%

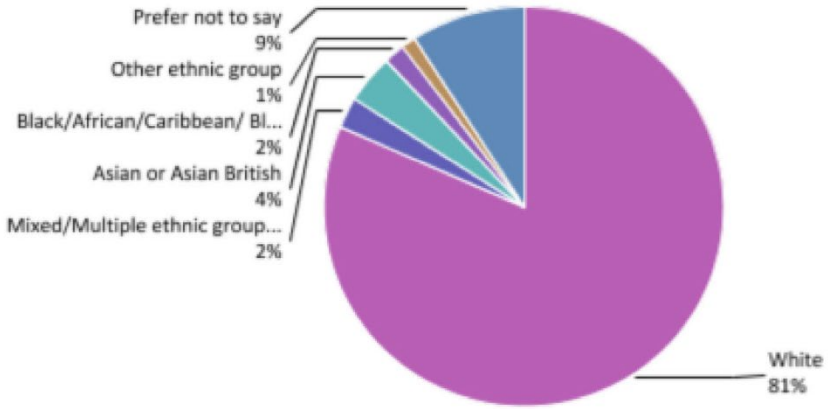
Base 2534, Not answered 3 (Valid response 100%)
Confidence Interval 2% at 95% confidence
*% - indicates percentage greater than 0 and less than 0.5



D3 - What is your ethnicity?

White	81%
Mixed/Multiple ethnic groups	2%
Asian or Asian British	4%
Black/African/Caribbean/ Black British	2%
Other ethnic group	1%
Prefer not to say	9%
Total	100%

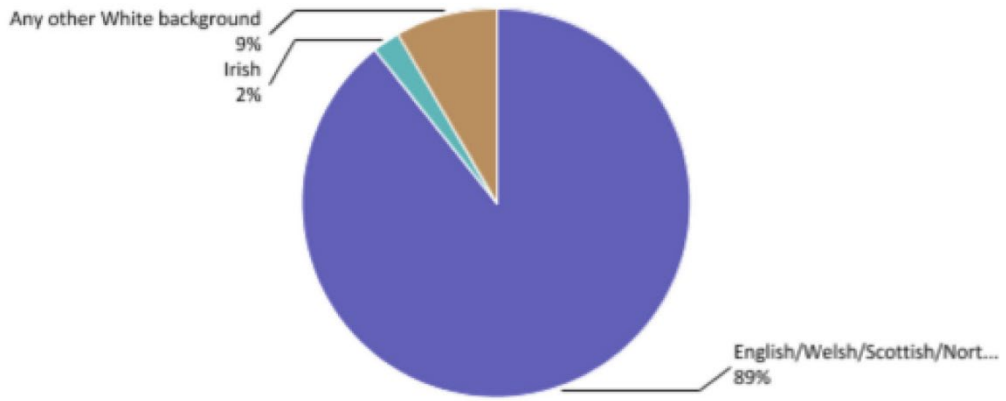
Base 2530, Not answered 7 (Valid response 100%)
Confidence Interval 2% at 95% confidence



D4 - Is that...?

English/Welsh/Scottish/Northern Irish/British	89%
Irish	2%
Any other White background	9%
Total	100%

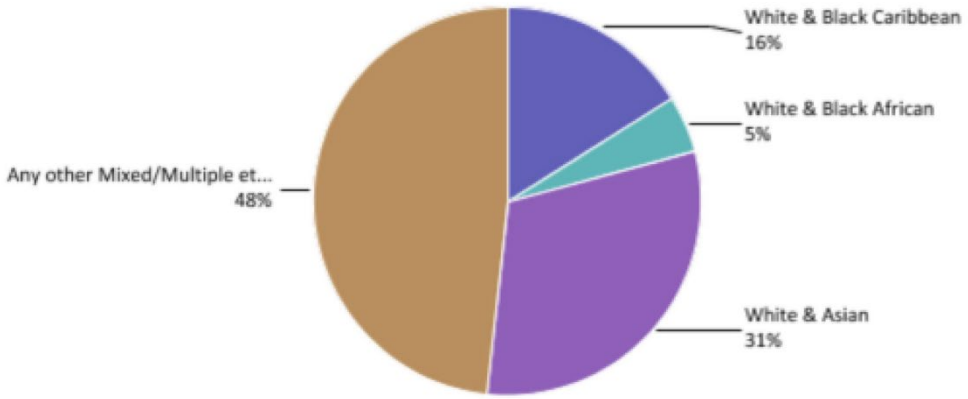
Base 2056, Not answered 5, Question not asked 476 (Valid response 81%)
Confidence Interval 2% at 95% confidence



D5 - Is that...?

White & Black Caribbean	16%
White & Black African	5%
White & Asian	31%
Any other Mixed/Multiple ethnic background	48%
Total	100%

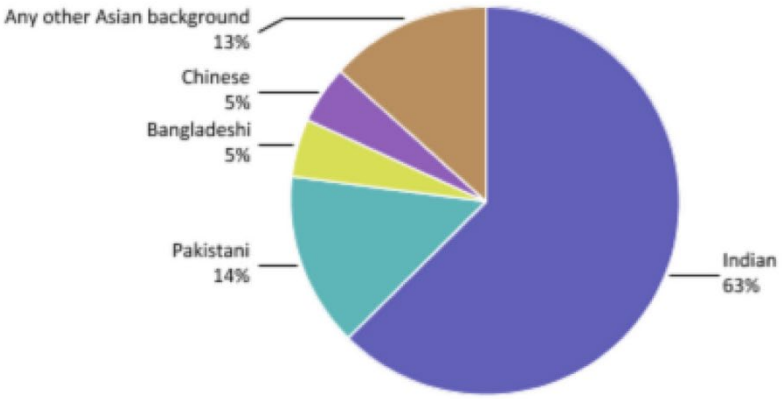
Base 62, Question not asked 2475 (Valid response 2%)
Confidence Interval 3% at 95% confidence



D6 - Is that...?

Indian	63%
Pakistani	14%
Bangladeshi	5%
Chinese	5%
Any other Asian background	13%
Total	100%

Base 104, Question not asked 2433 (Valid response 4%)
Confidence Interval 3% at 95% confidence

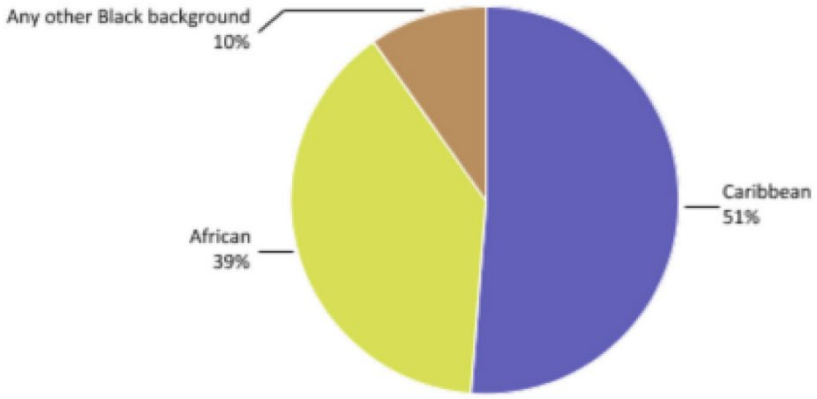


D7 - Is that...?

Caribbean	51%

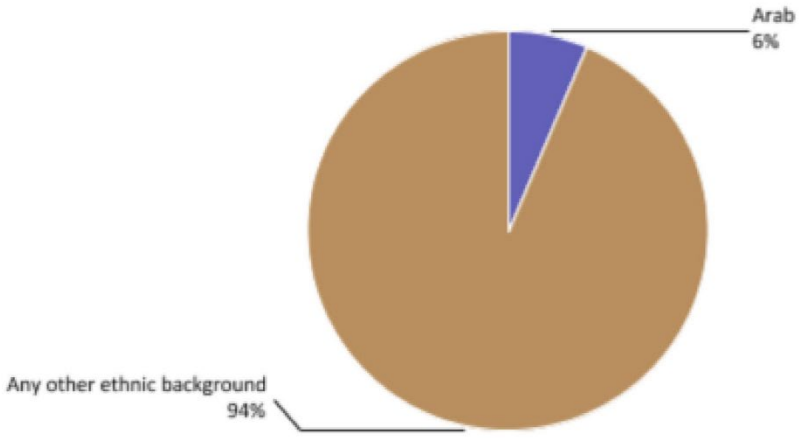
African	39%
Any other Black background	10%
Total	100%

Base 41, Question not asked 2496 (Valid response 2%)
Confidence Interval 3% at 95% confidence



D8 - Is that...?

Arab 6%
Any other ethnic background 94% Total 100%
Base 31, Question not asked 2506 (Valid response 1%)
Confidence Interval 4% at 95% confidence

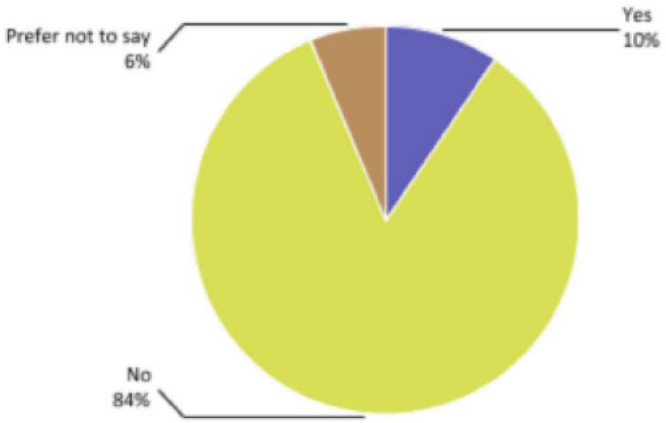


D9 - Do you consider yourself to have a disability?

Yes	10%
No	84%

Prefer not to say	6%
Total	100%

Base 2533, Not answered 4 (Valid response 100%)
Confidence Interval 1% at 95% confidence



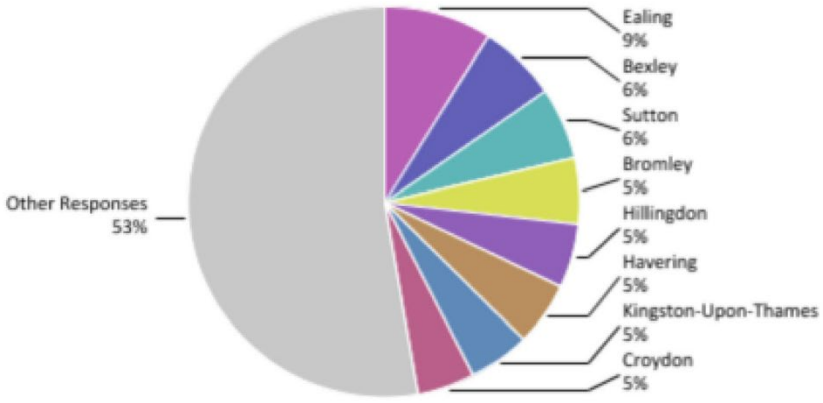
D10 - In which London Borough do you reside?

Ealing	9%
Bexley	6%
Sutton	6%
Bromley	5%
Hillingdon	5%
Havering	5%
Kingston-Upon-Thames	5%
Croydon	5%
Other responses	53%
Hide other responses	H
Richmond-Upon-Thames	4%
Merton	3%
Hounslow	3%
Redbridge	3%
Waltham Forest	3%
Barnet	3%
Wandsworth	3%

Greenwich	3%
Tower Hamlets	2%
Barking & Dagenham	2%
Lambeth	2%
City of Westminster	2%
Lewisham	2%
Hackney	2%
Southwark	2%
Harrow	2%
Haringey	2%
Newham	2%
Brent	2%
Camden	2%
City of London	1%
Hammersmith & Fulham	1%
Islington	1%
Kensington & Chelsea	1%

Total 100%

Base 2310, Not answered 227 (Valid response 91%)
Confidence Interval 1% at 95% confidence



METROPOLITAN POLICE

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

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	
Authority for Publication	This document can only be made public on the explicit Authority of either or a combination of the following Authorities: **1.** <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].
Information Security [Access Controls] And Personnel Security Clearance [Vetting] [MPS Vetting Policy takes precedence]	. 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: **1.** <u>For MPS personnel</u> - MPS Recruit Vetting (RV) or Counter-Terrorist Check (CTC) Additionally, access is also reliant on a **<u>direct need to know</u>** basis.
Physical Security [Storage/ offsite use of information] **[Remote Working – Working Away From the Office - WAFTO]**	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.]. 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: **1.** 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 theirclearance/ 'need to know' **2.** 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.). **3.** 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.

Electronic Security [Removable Media]	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.

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	
Movement [internal dispatch/ UK use of Post/ Courier Services]	The following despatched guidance/ instructions apply. Where this document has a GSC marking of **OFFICIAL** • **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**.
Movement [Use of Post/ Courier Services outside UK] This also includes the use of Fax machines	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

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/*