Template for Automatic Number Plate Recognition (ANPR) Infrastructure Development Privacy Impact Assessment

This template is provided to support the police service and other law enforcement agencies (LEA) to comply with their data protection obligations and meet individuals' expectations of privacy when developing new ANPR infrastructure. It has been developed to provide a consistent approach to the conduct of privacy impact assessments and support compliance with the Information Commissioner's Office (ICO) Conducting privacy impact assessments code of practice (February 2014).

Black Font: Suggested content to be included in the report
Red Font: Advice/ Guidance to assist completion of the relevant section.

Description of proposed ANPR development:

Provide an overview of the proposed ANPR development.

Privacy Impact Assessment completed by:

Date:

Part 1 Screening Questions

1	**Will the project involve the collection of new information about individuals?**
	Vehicle Registration Marks (VRM) will be obtained from locations not previously monitored by ANPR and therefore new information will be obtained from those locations.
2	**Will the project compel individuals to provide information about themselves?**
	The collection of VRM is automatic at the locations and therefore when an individual drives a vehicle at the new locations they could be considered as compelled to provide information. The Surveillance Camera Code describes overt surveillance in public places in pursuit of a legitimate aim and that meets a pressing need, as surveillance by consent. Such consent on the part of the community must be informed consent and not assumed by a system operator. Subject therefore to compliance with DPA and appropriate consideration of privacy, individuals can be considered to consent to the provision of information at the locations as opposed to being compelled to provide the information.
3	**Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**
	Whilst information from new locations will be disclosed it will only be disclosed to those organisations that currently have access to ANPR data.
4	**Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**
	The new ANPR infrastructure will provide ANPR data for the same purposes as for the data already obtained from ANPR systems. The developments will not alter the way in which it is used.
5	**Does the project involve you using new technology that might be perceived as being privacy intrusive? For biometrics or facial recognition.**
	The project does not involve the use of new technology that might be perceived as privacy intrusive.
6	**Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?**
	The purpose of the proposed development of infrastructure is in order to detect, deter, and disrupt criminality and therefore impact significantly on those involved in such activity.
7	**Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.**
	ANPR data is personal data since it can be combined with other information by an LEA to provide data relating to an individual. ANPR data does not however constitute private information since it is collected overtly in circumstances where there is no reasonable expectation of privacy. It therefore does not give rise to significant privacy concerns or expectations.
8	**Will the project require you to contact individuals in ways that they may find intrusive?**
	There is no requirement to contact individuals.

Part 2 Record of Privacy Impact Assessment (PIA) Process

Overview of the Proposed Development – Outlining the Pressing Social Need justifying the development of ANPR Infrastructure

(A key reference document is the Strategic assessment of policing challenges within an area should be structured to take account information relating to the following categories of strategic threat:

- National Security and counter terrorism,
- Serious, organised and major crime,
- Local crime,
- Community confidence and reassurance/ crime prevention and reduction.

It is important that an assessment against these high level categories is supported by evidence and information; a reference to these categories, in isolation, is unlikely to be sufficient to support the identification of a pressing social need for deployment of ANPR.

Provide a summary from the strategic assessment in this section.

In addition further information is required to establish a pressing social need for that threat to be countered by the deployment of ANPR. Whilst other factors may also be relevant this element of assessment requires consideration of the following factors, with appropriate analysis:

- The numbers of people that are, or could be affected by the issues identified within the strategic assessment.
- Whether those issues could lead to damage, distress or both and if so the nature and severity of those consequences.
- Any local views on the deployment of ANPR.
- Any wider societal views on the use of ANPR.
- The alternative tactical responses that may be available to meet the challenges that may be less or more intrusive than ANPR.
- How the use of ANPR will assist resolution of the issues identified.
- The scope of privacy intrusion – How many people does this affect?

All of the factors considered should be weighed against each other in determining whether it may be appropriate for ANPR to be deployed. It is essential that a pressing social need is identified for a deployment of new infrastructure or continue use of existing capability to be justified and for this to then be considered in the context of privacy.)

Provisions for Collection, Use and Deletion of ANPR data.

As a vehicle passes an ANPR camera, its registration number (VRM) is read and forwarded to a local database where it instantly checked against database records of vehicles of interest and stored to enable later research. If the number is for a vehicle of interest (VOI) details can be passed to Police officers who can intercept and stop a vehicle, check it for evidence and, where necessary, make arrests. In addition to the 'read' data images of the number plate (plate patch) and overview of the front of the car is obtained in most cases and forwarded to the local database.

In addition a copy of the read data together with the plate patch is forwarded to the National ANPR Data Centre (NADC) where details are also stored to enable later research. The VRM read by the ANPR camera is also checked against lists of VOI that have been placed on the NADC by other LEA. If the VRM is matched against any of those lists then the LEA submitting the list is also provided with details of the VRM read together with the time and location of the read.

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

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

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

ANPR data is retained both locally and nationally for a period of 2 years before it is deleted.

Consultation Requirements

Internal:

(can include informal discussions and e-mails. Project management meetings and discussion on agenda of other regular meetings)

Project team

Data Protection/ Information compliance officer – can provide specialist knowledge on privacy issues.

Information technology – can advise on security risks that may impact on security

ANPR Manager – can advise on specialist aspects of ANPR systems

Communications – PIA can assist in resolution of privacy concerns by providing clear information about a project and capability.

External:

The scope of external consultation should be assessed in the context of the development that is proposed. There are 2 main aims from external consultation. Firstly to enable understanding of the concerns of external stakeholders and secondly to improve transparency by making people aware of how ANPR is used.

The extent of consultation should be determined in relation to the assessment of the privacy related risks in the context of the location, the transient and resident populations. In most cases existing communication and consultation mechanisms within an LEA will be appropriate. These include all existing focus and advisory groups that support public engagement provide. The ICO Code indicates that "where possible, existing consultation tools should be used to gain a better understanding of privacy expectations and experiences." It is only in the largest planned developments that an alternative, more extensive approach may be required.

A record should be maintained of the consultation process.

Privacy Risks			
Risk	**Solution**	**Result**	**Evaluation**
The deployment of ANPR at a location is not proportionate	Assessment of 'Pressing Need' supported by a detailed strategic assessment, decisions taken following consultation and consideration of all issues.	Risk reduced	A robust assessment process for infrastructure development provides a proportionate response to the aims of the project taking account of any privacy concerns.
Individuals not involved in criminal activity consider the new ANPR deployments as unjustified intrusion on their privacy.	Transparency in regard to ANPR with provision of information concerning how it is used provide via Internet sites, written communication and trough appropriate signage. Access controls in place in accordance with NASP	Risk reduced	Increased awareness of how ANPR is used and the controls in place to prevent misuse will reduce concerns.
Action taken as a result of ANPR 'hits' from a camera may be seen as disproportionate.	Management controls in place to ensure use is in accordance with NASP. Robust process for managing lists of vehicles of interest to ensure that data for circulated vehicles remains accurate and relevant.	Risk reduced	Efficient business process will reduce the likelihood of inaccurate data and compliance with policy on use will ensure that use is proportionate.
Inappropriate sharing of data	Data is only shared and accessed in accordance with NASP. Provisions for monitoring and audit of data access and use in place.	Risk reduced	Compliance with business rules provides safeguards to prevent misuse and enable the benefits from the development to be realised.
Excessive data is collected	ANPR is only deployed where a pressing need has been identified. The continued requirement will be reviewed in accordance with NASP. Retention and disposal of data is in accordance with NASP.	Risk eliminated	Compliance with NASP ensures that data is collected and managed in accordance with agreed national standards.
Data is retained longer than necessary	Compliance with NASP regarding retention and disposal of data	Risk eliminated	Compliance with NASP ensures that data is collected and managed in accordance with agreed national standards.
Deployment will be considered disproportionate and subject to complaint to ICO.	Compliance with national guidance for the development of ANPR infrastructure. Decisions taken following strategic assessment taking	Risk accepted	Decisions regarding deployment are taken following proper assessment, nonetheless it is recognised that some may disagree with the

	account of identified privacy concerns identified through timely consultations with appropriate groups and individuals.		decisions and the opportunity for review by the ICO is an essential safeguard.
ICO may determine that deployment is inappropriate leading to sanctions.	Compliance with national guidance for the development of ANPR infrastructure. Decisions taken following strategic assessment taking account of identified privacy concerns identified through timely consultations with appropriate groups and individuals.	Risk reduced	A robust development process reduces the likelihood of ICO review concluding that the deployment of infrastructure at a location is inappropriate.
Any additional risks identified by the LEA.			

Privacy Risks Solution Approval		
Risk	**Approved Solution**	**Approved by**
The deployment of ANPR at a location is not proportionate	Assessment of 'Pressing Need' supported by a detailed strategic assessment, decisions taken following consultation and consideration of all issues.	
Individuals not involved in criminal activity consider the new ANPR deployments as unjustified intrusion on their privacy.	Transparency in regard to ANPR with provision of information concerning how it is used provide via Internet sites, written communication and trough appropriate signage. Access controls in place in accordance with NASP	
Action taken as a result of ANPR 'hits' from a camera may be seen as disproportionate.	Management controls in place to ensure use is in accordance with NASP. Robust process for managing lists of vehicles of interest to ensure that data for circulated vehicles remains accurate and relevant.	
Inappropriate sharing of data	Data is only shared and accessed in accordance with NASP. Provisions for monitoring and audit of data access and use in place.	
Excessive data is collected	ANPR is only deployed where a pressing need has been identified. The continued requirement will be reviewed in accordance with NASP. Retention and disposal of data is in accordance with NASP.	
Data is retained longer than necessary	Compliance with NASP regarding retention and disposal of data	
Deployment will be considered disproportionate and subject to complaint to ICO.	Compliance with national guidance for the development of ANPR infrastructure. Decisions taken following strategic assessment taking account of identified privacy concerns identified through timely consultations with appropriate groups and individuals.	
ICO may determine that deployment is inappropriate leading to sanctions.	Compliance with national guidance for the development of ANPR infrastructure. Decisions taken following strategic assessment taking account of identified privacy concerns identified through timely consultations with appropriate groups and individuals.	
Any additional risks identified by the LEA.		

Integration of Privacy Solutions into the Project		
Action to be taken	**Date for Completion**	**Allocated to**