<table>
<tr><th colspan="3">South Wales Police Data Protection Impact Assessment</th></tr>
<tr><td>Name of Project, Programme, Process or Policy:

Automated Facial Recognition (AFR)</td><td colspan="2">Details of personnel involved in undertaking the DPIA</td></tr>
<tr><td rowspan="5">Version 5.4

Date: 11/10/2018</td><td>Name:</td><td>Scott Lloyd</td></tr>
<tr><td>Rank:</td><td>Inspector</td></tr>
<tr><td>Department:</td><td>Corporate Development</td></tr>
<tr><td>Role:</td><td>Digital Services Division</td></tr>
<tr><td>Contact details:</td><td>X 70831</td></tr>
<tr><td colspan="3">Identify the need for a DPIA: Explain what the project aims to achieve, what the benefits will be to South Wales Police, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions). Remember a DPIA is an evolving document, so there probably will not be definitive answers to all these questions. Rather, it will identify issues and risk that may need solutions.</td></tr>
</table>

Version Control

Version	Date	Author	Purpose
V5.4	11/10/18	S.Lloyd	Original Publication

Table of Content

1. Introduction 4

2. Legislative Framework 8

3. Privacy Impact Screening Questions 18

4. Information Flow and Retention 19

5. Consultation 25

6. Data Protection Act Principles 28

7. Risk Identification and Reduction 39

8. Data Privacy Impact Assessment Sign-off 41

1. Introduction

South Wales Police (SWP) prides itself in keeping South Wales safe through the provision of a professional, proud and positive service that is the best at understanding and responding to needs of its communities.

The organisation is charged with reducing risk to the public; maximising the safety of its officers and staff; the arrest of offenders; gathering of intelligence; securing and preserving evidence in respect of those who choose to flout that risk; minimising disruption to our communities and enhancing trust and confidence of our organisation within those communities.

At any one time, people will be wanted for the commission of offences, be suspected of committing such offences or perhaps are about to commit offences that contradict the above standards and values. As an organisation, we also have responsibility for the prevention of the commission of offences.

Of course, it is accepted that offending will range in both type and seriousness, also that those suspected will also flout what may be seen as traditional means of detection - but the need exists to maintain the lowest numbers possible of persons who remain at large to deliver the safest environment.

In an austere climate, the challenges presented in locating and arresting offenders should rightly be challenged and with the assistance of technology, more enhanced and cost effective methods can be called upon to bring those responsible or suspected of offences more quickly to justice. Any project or set of new processes that involve exchanging personal information has the potential to give rise to privacy concerns from the public. This document looks to alleviate those concerns whilst embracing this new technology.

Technologies such as CCTV, ANPR and more recently Body Worn Video (BWV) have become more commonplace. Automated Facial Recognition (AFR) could be the next iterative step in the fight against criminality, reducing risk, protecting the vulnerable and keeping the public safe.

In embracing the technology, it is accepted that challenges lie ahead and this DPIA seeks to be organic as awareness and maturity grows with the system and indeed those charged with introducing and developing it - as the impact or the perception of impact upon the privacy of others should never be underestimated.

What is Automated Facial Recognition?

South Wales Police is leading UK policing in the deployment of Facial Recognition Software in both live environments and during slow time enquiries.

Facial recognition relies on physical features, when a face is captured by the technology it generates a biometric template.

There are two elements to the project:

AFR Locate: 'Live-time' deployment of AFR technology, which compares live camera feeds of faces against a predetermined watchlist in order to 'locate' persons of interest. This generates possible matches that are reviewed by the operator(s).

AFR Identify: 'Slow-time' application of AFR technology, comparing still images of unknown suspects and persons of interest , against a custody database of circa 460,000 images, and returning up to 200 results. These results are ranked based on the technology generating a 'similarity score' and are then reviewed by the operator, who decides whether a possible match is made and then return the information to the investigating officer.

When use AFR?

To Identify and Locate:

1. Individuals suspected of criminality and who are wanted by the courts and police.
2. Individuals who may pose a risk to themselves and others.
3. Individuals who may be vulnerable.
4. To effectively demonstrate the technology to the public and wider community to aid understanding, reassurance and to provide greater transparency.

Data protection impact assessment

Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.

A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.

A data protection impact assessment must include the following :-

(a) Describe the nature, scope, context and purposes of the processing

(b) Assess necessity, proportionality and compliance measures;

(c) Identify and assess risks to individuals; and

(d) Identify any additional measures to mitigate those risks.

Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing.

The aim of the DPIA is to show that AFR is compliant with the Data Protection Act 2018 (DPA), the General Data Protection Regulation (GDPR) and the European Convention of Human Rights (ECHR) as well as other associated statutes and directions. It is also to explain the extent of the use of the technology; limitations of that use; how data is captured, stored, processed and deleted; and analysis of the rights to privacy of citizens and the risks that this could impose on its introduction. The objective of the DPIA is to identify issue associated with such use.

It helps assess privacy risks to individuals in relation to the collection, use and disclosure of the information obtained from the technology. It helps identify privacy risks, foresees problems and brings forward solutions. The primary purpose is to demonstrate that this organisation acts responsibly in relation to the privacy of others whilst we engage in technologies that allow us to keep the communities of South Wales safe. The deliverables and benefits of undertaking a DPIA can be summarised as follows:

- The identification and management of risk against privacy
- Avoidance of unnecessary costs
- Prevention of inadequate solutions
- Avoiding loss of trust and reputation
- Informing citizens and partners of the organisation's communications strategy
- Meeting and exceeding legal requirements

Data sharing and testing must be undertaken within a clear legal framework with any intrusion upon an individuals' privacy kept to a minimum. By undertaking a DPIA we ensure this principle is met.

DPIA Process

The process for conducting a DPIA is described by the Information Commissioners Office (ICO) as a means to help systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of the accountability obligations under the GDPR, and when done properly helps assess and demonstrate how to comply with all of the data protection obligations.

It does not have to eradicate all risk, but should help minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what we want to achieve.

DPIAs are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects.

What is meant by privacy?

The Information Commissioner's Office Guide to completing a DPIA describes privacy in its broadest sense, as the right of an individual to be left alone. It can take two main forms and these can be subject to different types of intrusion;

1. Physical privacy - the ability of a person to maintain his or her own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference such as acts of surveillance or the taking of biometric information

2. Informational privacy – the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of message.

2. Legislative Framework

The legal framework for the use of AFR is summarised below:

- Common Law
- Human Rights Act 1998
- Data Protection Act 2018
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000

The use of AFR technologies is governed by a number of codes of practice including those applying to the police such as PACE. In particular the use of AFR is covered in the twelve principles laid down in the Surveillance Camera Code of Practice, to which the police must have regard when using such systems, as well as any other surveillance camera systems that relevant authorities operate. In addition, the Information Commissioner's Office (ICO)'s Code of Practice for surveillance cameras applies to their use by the police and other authorities.

The DPIA is a process, which helps organisations anticipate, and address the likely privacy impacts of projects in order that problems can be foreseen and solutions developed to ensure that concerns are addressed appropriately.

SWP is intent on introducing the concept of AFR into the operational policing environment in an incremental process so as to fully understand the methodology from simple to complex environments that enhances the information, identification and where necessary the evidential gathering processes against an individual(s).

It is accepted that civil rights groups have started to voice concerns over the invasion of privacy by this technology, particularly during live deployments.

SWP will adopt an incremental approach to AFR and its deployment, aware that the technology can be used not just to assist in identifying someone, but also that the possibility may exist in the longer term of interfaces with other technologies as such systems develop.

It therefore has the potential to fundamentally change policing practices and in doing so enables a user to secure information on an individual in a fashion not previously thought achievable.

General Legal Considerations

With the engagement and delivery of emerging technologies, no substantial legal difficulty is identified that would tend to advise on against use of such a system. The issue will be the manner in which the system is used or tasked; the retention, review and deletion of data recovered; any directed tasking of the system for overt and covert directed surveillance purposes as well as the ethical dilemmas and invasions of privacy counter arguments against such use. Justification, proportionality, legality, auditability and accountability, necessity and ethical arguments remain at the heart of this document.

We note that there is an opportunity to further strengthen the legislative framework and national governance for AFR when utilised by law enforcement.

In terms of highlighting the main legal considerations adopted and accepted at this early stage, it is accepted that the specific nature as well as evolving Standard Operating Procedures of a maturing system are still to be finalised, but the following are noteworthy:

Common Law

The police can, in fulfilling operational duties conduct themselves in a manner which is not contrary to law. These core principles include:

- Protecting life and property
- Preserving order

- Preventing the commission of offences
- Bringing offenders to justice

European Convention of Human Rights Act 1988

For the purposes of the European Convention of Human Rights (ECHR) and the Human Rights Act 1998, it is established that Police Forces and Local Authorities are able to utilise CCTV or other such recording systems in public areas for the purposes of public safety, and to investigate and prevention crime and disorder. The use of such recording technology however must be justifiable along with any rationale for the retention of any such data. The actions of the police must have a legitimate aim and the use of such equipment must be shown to be proportionate to achieving this.

Under this legislation, there are a number of 'Articles' to protect the rights of citizens. Some of these Articles are 'absolute' whereas others are 'qualified' and any interference with these is limited.

Interference with qualified rights is permissible only if:

- There is a clear legal basis for the interference with the qualified right that the public can understand, and
- The action/interference seeks to achieve a legitimate aim. Legitimate aims are set out in each article containing a qualified right and they vary from Article to Article, they include for example, the interests of National Security, the prevention of disorder or crime and public safety. Any interference with one of the rights contained in Articles 8-11 must fall under one of the permitted aims set out in the relevant article
- The action is necessary in a democratic society. This means that the action or interference must be in response to a pressing social need and should be assessed by demonstrating evidence of a level of severity or immediacy/unpredictability and alternatives should have been reviewed

Generally, any claims for the use of such a system would fall to be considered by the Courts as breaches of Article 8 of the ECHR namely the right to respect for private and family life, home and correspondence.

Article 8 is a 'qualified right' and therefore the processes which accompany the use of AFR will be required to address the 4 bullet points below and introduce suitable safeguards, associated with how we use the equipment and how the material is retained and for how long. Throughout, the principle objective is ensuring that any interference with the rights of parties can only be justified if it is:

- Necessary
- Proportionate
- In pursuit of a legitimate aim, and
- in accordance with the law

South Wales Police ensure compliance with the Human Rights legislation in respect of AFR.

Necessity

AFR meets the core principles in policing :

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

It is necessary to undertake the project in line with the Digital Services Division strategic intentions as well as operational objectives as defined with the AFR Project Initiation document. This will assist South Wales Police and key stakeholders to understand whether the use of AFR is a viable policing tactic.

The principal purpose of the technology is to identity and locate persons suspected of criminality as well as apprehending persons who are wanted on warrant. It will also prevent and reduce the incidence of crime. The technology will also have a significant role in assisting South Wales Police protect the most vulnerable persons in our community.

Proportionality

- It is considered appropriate to bring offenders to justice in an expeditious manner.

- Each deployment of AFR Locate should bring a benefit to the investigation or operation and should not be disproportionate or arbitrary.

- The fact that a suspected offence may be serious will not alone render intrusive actions proportionate.

Accountability

South Wales Police have developed a detailed governance structure to ensure that there is a sound accountability and engagement with key stakeholders. These include bi-monthly AFR Project Boards along with bi-monthly AFR Strategic Partnership Boards which involves key stakeholders and regulators.

South Wales Police are also represented at the 'Forensic Oversight Board' as detailed within the Home Office Biometric Strategy.

Home Office Biometric Strategy – Published June 2018

The strategy sets out how the Home Office and its partners currently use biometric data, and how they will approach future developments. It seeks to establish the overarching framework within which such considerations and decisions will be made.

South Wales Police have sought inclusion within the soon to be formed Oversight and Advisory Board as mentioned in Chapter 3 of the Strategy.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf

Recent claims against Chief Constables have tested the Police "rights" to take video or photographic evidence for intelligence purposes (Wood v Metropolitan Police Commissioner (2009) (CA). In essence, when the Police engage in the taking of photographs or video evidence in such scenarios, it can engage the Article 8(1) right. Therefore, any use of the system must be considered as against the three justifications above and subject of policy accordingly. Interestingly, such cases have focused more substantially on the retention periods for such data where it is not for criminal investigation or prosecution purposes. Further comment is made when considering MOPI guidelines and DPA legislation below.

In addition, Article 6 of the ECHR provides for the right to a fair trial. AFR will therefore need to have a procedure allowing for evidential recovery of data from the system compliant with CPIA and for the use of that data within criminal proceedings. It is clear that the use of

such a system could provide valuable evidence for use in criminal prosecutions albeit that there is currently no provision for the direct admissibility of such data. However, this justification may be closely scrutinised by a Court and it is essential that such data held will be retained in accordance with MOPI guidelines even where there is no clear evidence of an offence.

Other technological developments such as Body Worn Video recordings suggest guidelines of a 31-day retention limit if footage is not required for evidential purposes, increasing to 7 years or greater dependent upon the offence concerned.

http://swptools/GuidanceandProcedure/docs/Record%20Management/South%20Wales%20Police%20Record%20Retention%20Schedule.xls.

As the system embeds further, there is the intention that the technology becomes a fixed asset within custody suites. If this is to be the case, the privacy issues that arose from use of CCTV systems must also be considered, with the overarching principles of that use at the very least applicable when AFR also supports that technology.

Data Protection Act 2018

The Data Protection Act 2018 (DPA) is legislation that regulates the processing of personal data, including sensitive personal data, whether processed on a computer, CCTV, stills camera or indeed any other media. Any recorded image and audio recording from any device that can identify a particular person or learning about their activities is 'personal data' and therefore covered by the DPA. It is also appreciated that there are some exemptions from the Act in special circumstances. If the exemption applies dependent upon the circumstances, registration with the ICO, the granting of subject access, the provision of privacy notices and the non-disclosure of personal data to third parties can apply.

Principle 1 of the DPA (fair and lawful processing) requires that the data subject must be informed of:

1. The identity of the data controller
2. The purpose or purposes for which the material is intended to be processed and
3. Any further information that is necessary for processing to be fair

The Chief Constable has responsibility for controlling this information and is known as the Controller. It is appreciated that overt use of an Automated Facial Recognition system is likely to attract attention and therefore the force will consider an information release of the nature and extent of the system to aid public awareness. The principles of the DPA will also require:

- Staff have the necessary training to operate the systems including the location of any remote, fixed or flexible cameras and their remit
- All data is accessed, stored and used for a policing purpose
- Data is retained only for the periods established by MOPI and the procedure and is subject to review, retention and deletion protocols

The processing of personal data for AFR will be covered by both Part 3 of the DPA 2018 and under the General Data Protection Regulation (GDPR.)

Part 3 of the DPA 2018 makes a provision for processing personal data by competent authorities for law enforcement purposes.

It covers processing for the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Freedom of Information Act 2000

The Freedom of Information Act 2000 grants a general right of access to all types of recorded information held by public authorities, which includes information recorded by AFR.

The Act does however provide some specific exemptions to the requirements to disclose information, which must be applied on a case-by-case basis.

At the time of completion South Wales Police have received in excess of thirty Freedom of Information requests relating to AFR and have attempted to respond to each in a timely manner and in full.

Protection of Freedoms Act 2012

The requirements of the Protection of Freedom Act 2012 are covered by the Surveillance Camera Code of Practice 2013.

Surveillance Camera Code of Practice

An AFR system will need to be considered against this Code and the twelve guiding principles within it that ask:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once its purpose has been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim and a pressing need, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which matches against a reference database for matching purposes should be accurate and kept up to date.

This questionnaire has been completed and encapsulated having completed the Surveillance Assessment Tool (SAT).

Regulation of Investigatory Powers Act 2000

When the algorithm is deployed it is 'locked' so that it may not continue to learn and improve its ability to locate a particular face type.

The 'tasking' of the AFR system to find and identify key individuals will require consideration of the directed surveillance provisions of RIPA 2000. In this instance, the updating/inputting of a face/other data thereby identifying an individual may be considered 'tasking' the system to undertake surveillance for one or more individuals and therefore will require an Authority. As is suggested elsewhere in this document, we will seek to constantly refine and mature legal advice as more is learned of the technology.

Safeguards are considered under the principles of justification, proportionality, necessity and collateral intrusion as applied to RIPA 2000. Although AFR Locate is deployed in an overt manner, principles associate with RIPA are set as standards in order to demonstrate that surveillance principles have been considered.

Regulatory Investigative Powers Act 200 provides direction for covert surveillance but the guiding principles have been considered when deploying AFR Locate.

The Surveillance and Property Interference Codes of Practice (published 2014) relate to proportionality in respect to grading surveillance authorisations:

Section 3.5

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

Section 3.6

The following elements of proportionality should therefore be considered: • balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence; • explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others; • considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; • evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Home Office / NCPE (2005) Code of Practice on the Management of Police Information (MOPI)

This consists of both Guidance and a Code of Practice that directs how the police handle data coming into their possession will be retained for a 'police purpose' and this covers all situations where a police officer exercises a police power. It will include information gleaned from an AFR system.

The guidance further states that a 'policing purpose' includes:

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

These five purposes provide the legal basis for collecting, recording, evaluating, sharing and retaining police information.

The guidance provides a framework on how any data captured by police can be used and processed. In addition, it details the processes used by the police to initially retain, review and to ultimately dispose of data after the requisite timescales and circumstances have passed. The College of Policing (2013) APP on Information Management is an additional source of information.

Public Sector Equality Duty

The decision by the Force to use such a system is considered a function for the purposes of the Equality Act 2010. Forces must, therefore, be able to demonstrate due regard to the public sector equality duty by working with members of the public who reflect local diversity to ascertain any impact (whether positive or negative) that the use of such a system may have.

In order to ensure that the public are engaged in the use of the technology every opportunity has been taken to demonstrate its use, to include during Automatic Facial Recognition deployments. An example of this was the deployment at the Elvis Festival in September 17, which involved a secondary community engagement vehicle being deployed under the heading of 'How Elvis are you.' Consideration as to the impact of AFR has also been sought at the SWP Independent Ethics Committee and the Police Accountability and Legitimacy Group (PALG) the later focusing on the impact of AFR on persons with protected characteristics.

3. Privacy Impact Screening Questions

Q.1 Will the project involve the collection of new information about individuals? **Yes**

Q.2 Will the project compel individuals to provide information about themselves? **No**

Q.3 Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? **No** (save for access by academic partners for the sole purpose of evaluation)

Q.4 Will SWP be using information about individuals for a purpose it is not currently used for or in a way it is not currently used? **No**

Q.5 Does the project involve the SWP using new technology that might be perceived as being privacy intrusive, for example the use of biometrics or facial recognition? **Yes**

Q.6 Will the project result in SWP making decisions or taking action against individuals in ways that can have a significant impact on them? **Yes**

Q.7 Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations, for example health records, criminal records or other information that people would consider to be private? **Yes - the capture and potential retention facial images as set out under RIPA or other authority. The Home Office and SWP currently consider it as being lawful but some individuals have already argued that deployment of the technology lacks the necessary judicial oversight and in turn the use of AFR is unlawful.**

Q.8 Will the project require SWP to contact individuals in ways that they may find intrusive? **No**

4. Information Flow and Retention

Describe the information flows: You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

AFR Locate

Used to match real time CCTV to a watch list of persons of interest and alarm when detected.

The collection of personal information is via two CCTV cameras connected to the standalone laptop/server. The laptop is not connected to SWP ICT infrastructure and can be considered a 'black box' solution. The system 'extracts' a face from CCTV footage (known as a probe image) creates a biometric template and then compares it against a pre-defined watchlist, every candidate in the watchlist will also have a biometric template created. In doing so, the system does not save the live CCTV feed, only the face if a possible match is made against a candidate image along with a wider CCTV frame from which the probe image was extracted. The CCTV feed will itself be saved and that data management covered under a separate DPIA. The CCTV feed is recorded using Milestone Software and will be subject to automatic deletion after 31 days.

Not every person that is captured via the CCTV will be enrolled into the application. The face has to be of sufficient 'quality' to enrol into the application. The level of enrolment rate will be dependent on many factors, the significant of these include; crowd density, individual movements, face angle and lighting.

It is the intention during each deployment to allow the AFR application to enrol and therefore process as many individuals as possible, however it is worthy of note that processing that does not lead to an alert will be momentary.

The system has a built in audit trail functionality that ensures faces not matched against a candidate image are not retained within it.

The watchlist is created via a CSV file which is saved in a secure folder with the SWP ICT domain. The content of the folder is extracted into the application prior to deployment via an encrypted USB drive.

Watchlist data is saved within the system along with the accompanying metadata. This detail also forms part of the audit record. Watchlists and the associated metadata are manually added to the system during the day of deployment to ensure the information is as accurate as possible. If a deployment is over a number of days a bespoke watchlist will be added at the commencement of each day of deployment.

The watchlist is bespoke for each deployment, the rationale for the make-up of the watchlist is justified, proportionate and necessary with the nature of the watchlist recorded prior to each deployment.

Watchlists will wherever possible will be born from custody images to ensure consistency of image quality and ensure the legal basis for use as defined under PACE 1984.

Consideration has been given to ensure that only custody images taken in conjunction within an individual that was later convicted are utilised. Currently SWP custody images are recorded within the Niche RMS application. There is no way of automatically identifying images relating to an un-convicted process. As such a manual search is required to ascertain whether a custody image relates to an un-convicted process.

Typical deployments have resulted in watchlists of between 500 – 700 images. It has taken on average 3 minutes to manually confirm whether an image relates to a convicted individual. In order to fully redact the watchlist of un-convicted images this would take between 25 - 35 hours. It has been deemed as being impracticable at this stage to manually remove un-convicted custody images from AFR Locate watchlists.

The CSV file and encrypted dongle used to move the watchlist from SWP ICT systems into the AFR application are deleted immediately post upload into the AFR application.

The watchlist candidate images and related biometric template are deleted immediately post deployment and in any case within 24 hours.

Concerns have been raised by privacy experts that an individual may seek to enquire as to whether they have been included in a watchlist outside of the 24-hour retention period. Therefore, it has been deemed appropriate to be able to re-engineer watchlists. This can now be achieved via Niche RMS ‘back-end’ database by recording the nominal number of an individual extracted into a watchlist for on given date, this added functionality is available from October 2018.

During the life of the AFR project there has been considerable amount of attention placed on the retention period for the matched images. If a possible match is made three thumbnail images will be saved within the application along with the related metadata. The first is the candidate image, the second is the face extracted from the CCTV and the third being the CCTV frame from which the probe image was extracted.

At the commencement of the project the three images as identified above were saved for a period of 365 days in order to allow our academic partners opportunity to effectively scrutinise the technology and apply sufficient academic rigour to the project. As we have moved through the project this reduced to 3 months on the 22nd January 18. On the 5th March 2018 the retention period was reduced to 31 days.

The retention period for possible match alerts has again been considered and was reduced to 24 hours on the 25th June 2018.

Currently the possible match images and related biometric template are deleted immediately post deployment and in any case within 24 hours.

Post deployment and within 24 hours the match report to include the three thumbnail images are removed from the AFR application and saved in a shared folder located within SWP ICT domain. The images and match report are moved via an encrypted dongle which is then immediately deleted. As mentioned earlier once the match reports have been saved in the shared folder the three thumbnail images are deleted immediately and in any case within 24 hours with only the match report remaining. The match report is deleted after 31 days.

It will be appropriate at this point to highlight that the retention period around the CCTV feed to AFR remains unchanged.

AFR Locate deployments commenced on the 3rd June 2017 at the UEFA Champions League Final with a list of deployments detailed below.

As we are testing the technology South Wales Police have deployed in all event types ranging from high volume music and sporting events to indoor arenas.

There was a change in the AFR Algorithm deployed in late October 2017. Initial testing of the current algorithm would indicate it is far more accurate than the previous one deployed, being more capable at dealing with facial angle, pitch, yaw and partial facial captures.

The fact that the technology acts in a 'subtle manner' is not lost on anyone in SWP, to combat this we have derived a detailed communication strategy to support each deployment, more to follow on this later in the document.

Summary of retention period for AFR Locate

Watchlists – Deleted within 24 hrs (as of Oct 18 there is the ability to re-engineer watchlists for any given deployment)
Match Report – Three alert images deleted within 24 hrs / remaining log 31 days
Operator Logs – 31 days
CCTV feed – 31 days

What remains after 31 days?

AFR deployment register / AFR Locate deployment reports (neither of these documents include personal data.)

AFR Locate Deployments

UEFA Champions League Final - 31st May – 4th June 17
Elvis Festival - 23rd - 24th September 17
Op. Fulcrum - 19th October 2017
Joshua Fight - 28th October 17
Wales vs Australia - 11th November 17
Wales vs Georgia - 18th November 17

Wales vs NZ - 25th November 17
Wales vs SA - 2nd December 17
Kasabian Concert - 4th December 17
Gallagher Concert - 13th December 17
Op. Fulcrum - 22nd December 17
Op. Malecite - 23rd December 17
Royal Visit - 18th January 18
Wales vs Scotland - 3rd February 18
Wales vs Italy (UPSI Trial) - 11th March 18
Wales vs France - 17th March 18
DPTRE - 27th March 18
BBC Biggest Weekend - 26th – 27th May 18
Volvo Race - 28th May – 10th June 18 (6 days)
Beyoncé / Jay Z Concert - 6thJune 18
Rolling Stones Concert - 15th June 18
Ed Sheeran Concert - 21st - 24th June 18

AFR Identify

Used to compare a crime scene image (e.g. CCTV still) to a large database of images such as a custody set of images

Probe images (image of individual attempting to identify) will be obtained from a variety of sources, to include CCTV, BWV, jpeg, social media, etc and saved within SWP crime recording system (Niche RMS.)

During the life of the project consideration has been given to better equip officers in order to capture the best quality images available, work is currently ongoing in relation to realising this by allowing the community where possible to transfer images directly to SWP.

The watchlist for AFR Identify is made up from custody images, which are currently saved in Niche RMS. Upon go live for the AFR server a script was run against Niche RMS to bulk enrol the custody images into the AFR application. Again, consideration has been given to remove non-convicted images but at this stage is not possible due to the issues documented previously in this report.

Niche RMS is a collaborative crime recording system hosted by SWP but also utilised by Gwent with all custody images being accessible across both forces.

Currently there are circa 450k custody images within Niche RMS.

Every custody image relating to an individual will be imported into the AFR application, this is necessary because often the matched image may not be from the most recent custody image of an individual.

Post bulk upload candidate images will be uploaded into the application on a real time basis. When the individual has their custody image taken these will be ‘seen’ by the AFR application and ingested. Currently there is approximately a 5-minute lag between Niche RMS and the AFR application.

To ensure parity between the image library in Niche RMS and the AFR application each image is applied a hash value with the values being compared on a daily basis to identify any variance.

To that end when an individual successfully applies to SWP for a non-convicted custody process image to be deleted from Niche RMS the comparison of the hash values would effectively identify the inconsistency between the data sets and an alert email would be sent to the project team to ensure deletion from the AFR application.

Probe images will be imported into the application by the Identification team. If a probe image is of insufficient quality it will fail to enrol into the AFR application and as such will not be saved in the application.

When a probe is compared against the watchlist the probe image will be saved into the application and will be retained in line with the MOPI retention categories. A record of the search will be available within the audit log of the application, this will include the probe image but the relating candidate images are not saved as part of the audit log.

The only metadata to accompany the image making up the candidate list will be the Niche nominal number.

5. Consultation

Consultation requirements: Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. You can use consultation at any stage of the DPIA process.

A number of stakeholders have been engaged from the outset of this project to ensure legitimacy and transparency in terms of privacy and its potential impact upon the communities of South Wales. The following have already been consulted, but the list remains organic along with the DPIA itself as deployments mature and develop:

1. Information Commissioner's Office – Liaison and assistance on completion of the PIA as well as the additionality associated with the formal academic study over the implementation of the technology.
2. Defence Science and Technology Laboratory (DSTL) – With the provision of guidance on procurement, testing and deployment of the technology, along with advice around academic documentation supporting the proof of concept of the product. They remain a critical friend to the project.
3. Home Office Biometric Programme (HOBs) – Additional guidance in support of the above from the HOB lead on PIA's.
4. South Wales Police Independent Ethics Committee – early engagement over the concept of implementation and its engagement with privacy against the provision of safer communities.

5. The Metropolitan Police – Professional discussions around lessons learned over previous deployments, particularly the Notting Hill Carnival in the pursuit of a best practice model across forces.
6. Leicester Police – Professional discussions over their previous use of slow-time recognition functionality in the preparatory phase of our project implementation.
7. National Police Chiefs Council – Professional discussion and advice over the development of the project in its phases and the use of custody image.
8. The Surveillance Camera Commissioner – Professional discussion over project proposals and implementation.
9. The Biometrics Commissioner – Professional discussion over project proposals and implementation
10. The College of Policing – Professional discussion over deployment of an AFR APP
11. Police ICT Company – Professional discussions over system developments against a desired national rollout picture of the future.
12. The University Police Science Institute – Professional discussions integrating academic research into the policing technology, the ethical dilemmas associated with it and its deployment.
13. National Law Enforcement Database Programme (NLEDP) – Guidance in support of new platform anticipated October 2018.

A robust consultation strategy has ensured comprehensive feedback, commentary and support in the creating and quality control of the DPIA.

South Wales Police welcomes any feedback on the use of the technology. We are very much aware of the ethical considerations and debate that exist around its use. To that end we have ensured that the use of the technology along with numerous potential use case scenarios have been presented to the SWP Independent Ethics Committee (IEC). To date AFR has featured at four IEC meetings and is due to feature at the next IEC scheduled for September 2018.

Wider debate has been sought at the Surveillance Camera Commissioners Advisory Counsel held on the 22nd May 2018. In attendance were representatives from Liberty and Big Brother Watch. South Wales Police were invited to attend this meeting and provide an overview of the use of the technology. Concerns over its use were raised by both representatives from Big Brother Watch and Liberty. Time was taken after this meeting to discuss the use of the technology in more detail with representatives from Big Brother Watch.

Local accountability is delivered through an established governance structure. Weekly AFR tactical meetings are carried out by the Project team with a post event debrief completed after each AFR Locate deployment. Tactical issues of note are delivered to bi-monthly

AFR Project Boards which have more recently been replaced with a Bronze Digital Services Division Project Board, any issues from here are escalated to Silver and Gold meetings.

In parallel with the internal goverance is the AFR Strategic Partnership Board where the identified partners will engage. These currently sit quarterly with the next meeting due to take place at the end of July 2018. These meetings have often proved difficult for individuals to attend with people preferring to 'dial-in.' It is felt that the volume of engagement has often been hampered by the dial-in numbers and as such an alternative more central venue in London for the next meeting has been sought.

AFR Locate

The operational imperative to deploy the technique as part of the control strategy for a high risk, high profile event has wherever possible involved the communities of SWP. A prime example of this would be the deployment at the Elvis Festival in Porthcawl in September 2017 where a secondary engagement AFR vehicle was deployed. During this deployment the community were invited to interact with the technology and ask any questions they felt relevant. An engagement vehicle has also been deployed at every Basic Command Unit (BCU) Open Day in 2017 with future deployments planned in 2018.

Use of AFR Locate has received widespread publicity through the communication strategy advertising the tactic in advance of deployment and via trade literature advertising the commercial deployment. This approach will also assist academic research, as the reception of the tactic will form part of the review to be undertaken in support of the use of technology.

The communication strategy seeks to inform the public of the proposed use, its potential for impact on privacy and the proportionality of that impact as opposed to arguably more intrusive, traditional tactics.

Social Media has been used extensively to inform the community of each deployment. Where possible the location of the vehicle has also been advertised, with the public invited to 'take a look' at the technology. Social media has also been used by both the Project team and Chief Officers to participate in a healthy debate over the necessity and ethicacy of its use.

Academic support will be utilised to garner wider public opinion and the tactical use will be supported by electronic and paper leaflets explaining its use and what (if any) data will be recorded. Vehicles will also advertise electronic means of querying operational deployments.

In addition to the above, the privacy design features outlined elsewhere in this document will form part of the review and development of this DPIA to ensure protection afforded to processing data secured by this technology.

South Wales Police will ensure hat on the date of deployments notices identifying the use of the technology extend beyond the reach of the CCTV camera feed.

Privacy notices will be available for all individuals that are engaged as a result of a 'positive alert' along with being available to the wider general public.

AFR Identify

Robust communication strategy has been developed to identify hard to reach groups. Community engagement via four BCU open days.

Internal SMT engagement via attendance at four SMT Management meetings. Wider BCU engagement to include supervisors and BCU Local Intelligence Officers has been completed.

6. Data Protection Act Principles

Data Protection Act Principle 1

The processing of personal data for any of the law enforcement purposes must be lawful and fair, and only 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

b, the processing is necessary for the performance of a task carried out for that purpose by a competent authority

1.1 Why is the personal data being collected used, disseminated, or maintained?	The personal data will be imagery and the metadata associated with it, to include names, dates of birth, warning markers, method of disposal, the owner/originator and a reference number.
1.2 Where is the information collected from, how, and by whom?	From a series of non-networked systems and varying law enforcement databases. Personal data will be obtained from Niche RMS.
1.3 If collected by an organisation on behalf of the SWP Home Office, what is the relationship and authority/control the Home Office has over the organisation? Who is the Data Controller and Data Processor? Is a formal agreement in place to regulate this relationship?	Initially not, but expectations are that the system will develop at which time more formal agreements will need to be in place to regulate practices.
1.4 How will you tell individuals about the use of their personal data? Do you need to amend your privacy notices? Is this covered by the Home Office Personal Information Charter?	Initial deployment of this tactic will be an overt process supported by a communications strategy. Privacy notices have already been amended and distributed as well as being located on the SWP website.
1.5 Have you established which conditions for processing apply?	It is important to point out that the primary purpose for processing is for law enforcement as detailed within Part 3 of the Data Protection Act 2018. These will include:- Prevention, investigation, detection or prosecution of criminal offences and the prevention of threats to public security. It is also realised that biometric data such as facial images is subject to conditions with regard to sensitive data. The conditions relied upon for processing sensitive data include:- Judicial and Statutory purposes Administration of justice Safeguarding of children and of individuals of risk When a court acts in its judicial capacity Preventing fraud Research or statistical purposes

	It is considered that the identified processing of sensitive information is strictly necessary and there is a pressing social need which cannot reasonable be achieved through less intrusive means. The pressing social need seems to concern the weight and importance of the aims pursued. Over the life of the project and at any one time SWP is seeking to arrest (where the necessity test is made out) 350 individuals wanted on warrant and 350 individuals suspected of criminality. In order to best serve the community and in particular the victims, realising swift justice is a considerable aim. It would be almost impossible for any one police officer to be able to effectively remember and identify several hundreds of individuals from their face alone; use of AFR Locate assists the front line officer in providing a much smaller pool of individuals to scrutinise. Of course the same aim could be achieved by training dozens of officers, all to remember an equal split of the identified persons, this of course would not be an effective use of resources. Likewise for AFR Identify, there are other more traditional ways of identifying persons suspected of commiting a criminal offence. An image of the suspect could be shared with colleagues, circulated on social and national media. It is probably prudent at this stage to point out like other Police forces across the UK, SWP front line officers are generally very young in service, these officers would normally deal with the majority of crime where a suspect has been identified. The ability of young in service officers to recognise historical offenders may be limited, which would naturally result in suspect images being circulated more wider than ever before. It is believed that the use of AFR Identify is far less intrusive in identifying a suspect than employing traditional methods.

	Data may also be processed under the GDPR, for example missing persons; these include:- Consent – this has been considered, but is not applicable in the majority cases. The below conditions are relevant:- Public task – Article 6 1 (e) Vital Interests – Article 6 1(d) to help protect the most vulnerable in our communities Schedule 8 4(1) Safeguarding of children and individuals at risk
1.6 If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	Consent would be sought from the next of kin, carers of individuals reported missing, or who suffer with mental health issues on the rare occasions where Public Task and Vital interest do not apply. If consent is withheld or withdrawn, traditional policing methods would be employed to identify and locate the individual.
1.7 What information is collected, used, disseminated, or maintained in the system?	AFR Identify - Custody nominal images and probe images (to include Nominal naming convention.) AFR Locate - Watchlist information will realise matches to systems and databases to include false positives, the operator details and an audit log.
1.8 Is there a specific legal power that enables the gathering and use of the information? Does the power mandate the collection of the data or merely permit it?	The gathering of the information sought is in support of that that provides for the investigation of offences and the prosecution of offenders Police and Criminal Evidence Act (PACE) 1986.
1.9 Is there a specific business purpose that requires the use of this information?	Policing purposes generally – in assisting in the location and identification of individuals. AFR Locate will assist in SWP becoming more efficient and effective in locating persons of interest. These individuals could be persons wanted on suspicion for an offence, wanted on warrant, vulnerable persons and other persons where intelligence is required.

	AFR Identify will assist when there is a digital image of a person obtained, primarily in connection with a crime and their identity is sought. This will allow SWP to become more efficient in comparing this image against our custody database. Current research would suggest that offending is local and repeat and as such comparing suspect images against our custody database is considered a relevant tactic when trying to identify an individual.
1.10 Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?	Aside from the risks towards an individual, mitigation is realised with the operating system being password encrypted when at rest. When engaged, only trained users will be able to access the system through a single sign on password. Transfer of data is realised by an encrypted dongle/USB drive. When not in operational use, the system will be securely stored.
1.11 Human Rights Act: Will your actions interfere with the right to privacy under Article 8? Have you identified the social need and aims of the project? Are your actions a proportionate response to the social need?	Privacy is engaged, but only to the extent that the justified, proportionate, legal, auditable and necessary intrusion is allowed in relation to the investigation of offences, the prevention of crime and the investigations into missing person and safeguarding enquiries allow. As the system progresses, CCTV feeds will only take place from public areas so no collateral intrusions into wider private lives is anticipated. Wherever possible custody nominal images will be used to form the candidate list.
Principle 2: The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate and must not further processed in a manner that is incompatible with that the purpose for which it was collected.	
2.1 What are the main uses of the information? Does your project plan cover all of the purposes for processing personal data?	The main purpose of the use is for intelligence and information to be used to identify and thereby arrest offenders. The existence of the technology to deter the commission of offences is also accepted.

	AFR Locate will involve enrolling images of known individuals into a watchlist in order to locate them. Once located this may then involve a further interaction taking place between the identified individuals and an employee of SWP. There will be times when there is no intervention between the identified individual with this sighting being used for intelligence purposes only. AFR Identify will be used to compare digital images both still and moving against SWP custody database in order to identify them.
2.2 Have you identified potential new purposes as the scope of the project expands?	Yes, early considerations suggest that use of the product will diversify as the relationship with it matures. Future developments can potentially interface with other data assets.
2.3 Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?	Mitigation from the outset was secured by the provision of a non-networked solution, thereby eliminating any web application vulnerabilities. An operator cannot access any stored data, only another with 'adminstrator' level access to evaluate and prevent deletion control. Operators will be appropriately vetted to include sharing with third parties such as UPSI in the provision of academic review through an SLA still in the process of being developed. Data transfer issues have already been dealt with and retention will be compliant with MOPI requirements. Intervention teams will be in possession of an application that secures data onto a receiving device.
Principle 3: **Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.**	
3.1 Is the quality of the information good enough for the purposes it is used?	Yes, initial user acceptance testing supports this view.

3.2 Which personal data could you not use, without compromising the needs of the project?	None, the use of data and its associated metadata is key to the process – reinforcing the positive principles associated with the deployment.
Principle 4: **Personal data shall be accurate and, where necessary, kept up to date.**	
4.1 If you are procuring new software does it allow you to amend data when necessary?	Yes, the software allows for constant review and update
4.2 How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Data will be checked against core SWP databases, managed in accordance with MOPI standards. Proof of concept testing may realise the inclusion of non UK based data (Europol) who will be asked to assure standards are at least of the governing UK standard or its equivalent
Principle 5 **Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.**	
5.1 What retention periods are suitable for the personal data you will be processing?	AFR Locate CCTV Feed – not retained within application and subject to own PIA – currently retained for 31 days. Watchlist images and biometric template – deleted immediately post deployment and in any case within 24 hours Matched alert images (false and true positive) and biometric template – deleted immediately post deployment and in any case within 24 hours Non-matched images – immediately deleted Associated matched alerts metadata - currently retained for 31 days Operator Logs – currently retained for 31 days AFR Identify

	Watchlist Images and biometric template – PACE retention period Probe images – MOPI retention period depending on suspected offence All personal data will be stored in accordance with MOPI standards – tier 1 for 31 days, tier 2 for 6 years plus 1, with tier 3 retained for one hundred years.
5.2 Are you procuring software that will allow you to delete information in line with your retention periods?	Yes, software will manually feed data from another database that will itself be MOPI compliant in terms of retention and deletion requirements. It will require a manual intervention for compliance in the first instance, thereafter the compliance will be automated by the host database upon full integration. A designed compliance solution has been realised for AFR Identify by hashing the watchlist library to ensure parity with the custody image database.
5.3 Is the information deleted in a secure manner that is compliant with HMG policies once the retention period is over? If so, how?	This is managed through existing protocols. AFR will not own the databases, but be a customer of them in the receipt of images and metadata provided by others in this case
5.4 What are the risks associated with how long data is retained and how they might be mitigated?	The risk is held by the MOPI compliant database, that feeds a non-integrated solution. Phase 2 of the project will realise integration that can ensure greater compliance. The proposed academic exemption is again worthy of mention at this point.
Part 3, Chapter 3 Section 45 **States that a data subject is entitled to obtain from the Controller confirmation as to whether or not personal data concerning him or her is being processed, and where that is the case, access to the personal data**	
6.1 Will the systems you are putting in place allow you to respond to subject access requests more easily?	AFR Identify allows the searching of the database via the unique nominal number applied to every image.

	AFR Locate watchlist entries are accompanied with the name of the individual which could be searched upon request. The audit trail functionality would be more FOI suited because we would be able to realise the number of matches secured as opposed to the process of direct personal data to realise a named identification.
Principle 6 **Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.**	
7.1 Who will have access to the system? Please provide role and responsibilities.	Two types of access will be available to the system – 'user' and 'administrator' access levels.
7.2 What level of security clearance is required to gain access to the system?	Operating staff and academic partners will all be vetted and cleared to at least MV/SC level.
7.3 Does the system use 'roles' to assign privileges to users of the system?	Yes, see above.
7.4 How is access granted to the system?	With the authority of an administrator upon completion of training.
7.5 How are the actual assignments of roles and rules verified?	They are verified through project management protocols.
7.6 How is this data logged and how is this reported to prevent misuse of data?	The system has an in built and robust audit file log CSV file (hashed).
7.7 What training is provided to cover appropriate use and basic security to users? How is the training refreshed? Is the training tiered?	Two days 'administrator' and half day 'user' training is provided, with MOPI awareness to both. Refresher training is planned in due course
7.8 Has or is the system going to be formally accredited using HMG standards to process and store the information, if so who is the accreditation authority (person/organisation)?	The initial deployments will be under 'proof of concept' protocols, with liaison with HMG, DSTL and HOBs from the outset to include academic research support prior to any decisions being made over accreditation. Liaison continues also with the SWP FISO, SIRO and ICO.
7.9 Given access and security controls, what privacy risks were identified and how might they be mitigated?	Each operator will be given a user name and password which they will be forced to change on initial use of the system ('Active Directory'

	strength of eight characters to include upper and lower case as well as being alpha numeric. Local network passwords are security protected. The system is non-networked and non-configured to extend to the cellular network – essentially an additional geographical protection.
Transfers of personal data to third parties or international organisations Part 3, Chapter 5, Section 73	
8.1 Will the project require you to transfer data outside of the EEA?	No. Some data will be cloud based (evidence.com) a data centre located in the UK
8.2 If you will be making transfers, how will you ensure that the data is adequately protected?	Technically it is never transferred as the data is placed into a 'viewing pot', the audit functionality adds an additional layer. An information sharing agreement will exist between SWP and the Universities Police Science Institute (UPSI) attached to the University of South Wales over the academic research. The information we are sharing with academic partners would include access to the audit and operator log from the Automatic Facial Recognition deployments. This would include the related metadata and three thumbnail matched images. We would also provide UPSI with the wider details of the deployment to include watchlist rationale and size. Full watchlist content has not be shared with UPSI.
9 Internal sharing within the Home Office	
9.1 With which parts of the Home Office is the information shared, what information is shared and for what purpose?	It could be shared with HOBs and Defence Science and Technology Laboratory (DSTL) as part of the wider academic evaluation over the proof of concept matters within the project and the rollout across UK
9.2 How is the information processed or disclosed?	It could be disclosed via evidence.com or another secured medium – purely for the purposes of research, not law enforcement.
9.3 What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?	The only increased risk would be further disclosure by the Home Office, further that it is proposed to retain a data set purely for the purpose of the academic research so as to compare like for like as opposed to returning to additional data and a further, less necessary, intrusion upon privacy for the same purpose.

10. External sharing and disclosure (If you have already completed a HO Data sharing toolkit then please attach and leave these questions blank).	
10.1 With which external organisation(s) is the information shared, what information is shared, and for what purpose? Has the Home Office specifically asked suppliers to undertake PIAs?	As above, the only external organisation to receive data is UPSI for the purpose in a pre-agreed academic evaluation of the proof of concept to support HOBs and DSTL. Enquiries will determine whether a DPIA exists, or if one is therefore required.
10.2 Is the sharing of personal information outside the Home Office compatible with the original collection? If so, is it addressed in a data-sharing agreement? If so, please describe.	A service level agreement already exists with UPSI over the handling of personal data for the purposes of academic evaluation of policing matters.
10.3 How is personal information shared outside the Home Office and what security measures, compliance and governance issued safeguard its transmission?	Only used by vetted partners in a well-established relationship between SWP and UPSI.
10.4 Is a MoU in place for the Home Office to verify that an external organisation has adequate security controls in place to safeguard information?	Yes
10.5 Given the external sharing, what are the privacy risks and how might they be mitigated?	Again through the sole use of vetted staff attached to UPSI
11 Notice	
11.1 Do individuals have an opportunity and/or right to decline to disclose or share information?	Yes – during AFR Locate deployments SWP will ensure that we advertise the use of the technology in areas that extend beyond the reach of the CCTV feed cameras.
11.2 Do individuals have an opportunity to consent to particular uses of the information, and how?	On most occasions no, but as identified above consent could be provided by NOK with regards to children or Mispers who lack mental capacity.
11.3 How could risks associated with individuals being unaware of the collection be mitigated?	Through the provision of a detailed media strategy prior to deployment and a multi-layered approach that has involved direct messaging to the clubs involved, National and local media, social media and signage attached to vehicles as well as static deployments. This is not a covert tactic.

	Privacy notices will be available during AFR Locate deployments and offered to all persons where an AFR engagement is made.
12 Access, Redress and Correction.	
12.1 How are individuals notified of the procedures for correcting their information?	Not applicable – human error is the only potential at this time with a human eye currently acting as a stop-gap. Email messaging to advise of an error can be acted upon. Full integration would further reduce this risk
12.2 If no formal redress is provided, what alternatives are available to the individual?	Generic email address is established to deal with any operational policing AFR concerns.
12.3 What are the privacy risks associated with redress and how might they be mitigated?	There are none as there is no redress in this particular set of circumstances.
Aggregation of Data	
13.1 Will the wider sharing or aggregation of data held pose a risk of injustice to groups or individuals?	Yes, potentially – but no more so than present practices would equally allow. SLAs mitigate the risk but can never fully remove it.

7. Risk Identification and Reduction

Processing Risks	Risk reduction
An individual who has been identified via an alert and intervention has taken place and wants to complain	To date no person has complained about the use of the technology and no person who has been stopped as a result of an alert has complained. To that end it is not deemed necessary to keep watchlists for more than 24 hours. As of Oct 18 watchlists can now be re-engineered via Niche RMS 'back end' database should there be a need to recreate a watchlist for any given deployment. Privacy notices are offered to all persons where and AFR intervention has taken place which will include contact email. Officers are encouraged to obtain and record details of all persons that have resulted from an AFR intervention.

AFR Locate Intervention	Where AFR locate identifies a person as an individual who is subsequently confirmed as being wanted on warrant or suspect for a criminal offence it has not been deemed necessary to retain the probe image for longer than 24 hrs as the individuals identity will be subject to existing biometric procedures as defined by PACE 1984. Where an 'incorrect identification' is confirmed by human intervention officers are encouraged to record the individuals contact details for an audit trail, in the event that a complaint or Data Protection Subject Access request is made.
Unlawful arrest	Intervention officers will ultimately use traditional policing methods to ascertain an individuals identity before an arrest is justified.
Data Accuracy (latency)	Watchlists wherever possible will be complied on the day of deployment and will be bespoke for each day of deployment. The project team will ensure the correct formatting and inputting procedures are followed.
Watchlists	Operators will not have access to the watchlist data.
AFR Locate equipment not functioning	During project phase a member of the DSD department who has received 'enhanced' training will be available during each deployment. A false positive rate of 1 in 1000 or less will be maintained by amending deployment settings. Operator logs will be completed for each deployment which will be used to identify the volume of alerts.
False positive may lead to unwarranted intervention	The operator will review all alerts prior to any intervention with the final decision to intervene resting with the intervention officer.
Retention compliance	DSD department will ensure compliance with the identified retention periods.
Public Trust and Confidence	Stakeholder engagement and governance has been established. Media strategy has been developed and amended. Third party media engagement has been approved. AFR documentation and deployment register to feature on SWP AFR web page.

8. Data Privacy Impact Assessment Sign-Off

Person completing the DPIA	Name (in capitals)	**SCOTT LLOYD** **Inspector**
	Date:	**11/10/2018**
Approval Signature (Approval will be required by either the Senior Responsible Officer (SRO)/ the Information Asset Owner (IAO) or Head of Unit (HoU))	Signed:	
	Name (in capitals)	**RICHARD LEWIS** **Deputy Chief Constable**
	Date:	**11/10/2018**