

DRAFT South Wales Police Privacy Impact Assessment

Name of Project, Programme, Process or Policy:	Details of personnel involved in undertaking the PIA	
Version 4.0 Date: 12/02/2018	Name:	Scott Lloyd
	Rank:	Inspector
	Department:	Corporate Development
	Role:	Project Fusion
	Contact details:	X 70831
<p>Identify the need for a PIA: 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 PIA was identified (this can draw on your answers to the screening questions). Remember a PIA 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.</p>		

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) is 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 PIA 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?

AFR computer based application, an algorithm that is potentially capable of assisting in the identification of a person from a face/digital image/video frame or indeed analysing the same from another such product. That product can then typically be extended for use in other biometric or conventional databases – it has even begun to emerge commercially in identification and marketing campaigns.

Most are done through examination of facial features or points of a face and their position relative to each other against a dataset of a stored, primary image. It is in itself an emerging science with systems developing rapidly in relative short timescales. Errors have occurred in the developing technology, with differing products in the marketplace offering varying solutions – some more accurately than others. A significant advantage remains however in that it does not require the co-operation of a subject to provide results, with systems already employed around the world that identify faces in a crowded environment with recognised persons unaware of their recognition – and therein lies the dichotomy of risk against opportunity.

A clear challenge will be to ensure wherever possible that the best dataset available is adopted or that comparison is made against the most standardised set possible.

Why use AFR?

The primary use of AFR will be the prevention and detection of crime. Specifically, an enhanced and modern working arrangement that seeks to increase crime detection rates, increase and improve intelligence, assist criminal justice partner agencies in delivering best evidence, reduce officer report writing time as well as court appearances, ensure its use is in compliance with relevant legislation and to increase control of any digital evidence as an auditable crime exhibit.

The aim of the PIA is to show that AFR is compliant with the Data Protection Act 1998 (DPA) 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 PIA is to identify issues 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 PIA 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 PIA we ensure this principle is met.

PIA Process

The process for conducting a PIA is described by the Information Commissioners Office (ICO) as an initial assessment or screening process, which examines the project at an early stage, assessing privacy risks and decides which level of assessment is necessary. Then, conduct either a small scale PIA (a less formalised document with an information gathering and analysis phase) or a full-scale PIA (a more in-depth assessment and analysis of privacy risks and liabilities to include a need to identify stakeholders, consult widely with them on privacy concerns and bring forward solutions to accept, mitigate, transfer or avoid them). This report is considered a full PIA.

The ICO also suggests a timetable for reviewing actions taken as a result of the PIA and examines their effectiveness as well as looking at new aspects of the project and assesses whether they should result in an updated PIA.

What is meant by privacy?

The Information Commissioner's Office [Conducting Privacy Impact Assessments Code of Practice](#) 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 messages

The PIA 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 may start to voice concerns over the invasion of privacy by this technology.

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 an user to secure information on an individual in a fashion not previously thought achievable.

Standard Operating Procedures

The strategic aim of the AFR SOP is to provide clear guidance to all police officers and staff when accessing the application in order to deliver a service that reflects our mission statement to keep South Wales safe.

Insert SOP here

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.

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:

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 3 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
- In pursuit of a legitimate aim, and
- In accordance with the law

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.

Ethical questions emerge constantly with such new technologies and at the time of writing this document queries persist in terms of data retained for the purpose of training and whether such retained data is less intrusive than a second sweep with twice the intrusion to deliver the primary need. Again, directions will be constantly reviewed under this and related policy documents

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 1998

The Data Protection Act 1998 (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 Data 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

Crime Procedure and Investigations Act 1996

The ACPO (2007) Practice Advice on Police Use generated incidents Section 1.2 Criminal Justice Disclosure

[http://www.cps.gov.uk/legal/d to g/disclosure manual/disclosure manual chapter1/](http://www.cps.gov.uk/legal/d%20to%20g/disclosure%20manual/disclosure%20manual%20chapter1/) contains further information about this requirement.

Police generated incidents should be accompanied by a full audit trail, from the point of report through the whole management process to include passing to prosecution or defence authorities or any supervised viewing takes place.

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.

Regulation of Investigatory Powers Act 2000

It is understood that an AFR system will require the input of data 'faces' as well as metadata associated with them to allow for a systematic 'recognition' of an image via algorithmic support from the system. It can be argued that the systems, for want of a better expression 'learns' a face with repeated consideration which tends to make it more likely that the system will then locate the face searched for within an otherwise anonymous crowded environment.

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.

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. What is the system for and do you review its use?
2. Have you carried out a Privacy Impact Assessment and is it published?
3. Do you have signage in place to say surveillance is taking place and is there a published point of contact for people to raise queries or complaints with?
4. Who is responsible for your system and are your staff aware of their responsibilities?
5. Do you have clear policies and procedures in place and do your staff know what your policies and procedures are?
6. How long do you keep images/information and how do you make sure images/information is deleted once they are no longer needed?

7. Do you have a policy on who has access to the stored information and do you have a policy on disclosure of information?
8. Do you follow any recognised operational or technical standards?
9. Do you make sure that the images captured by your system are caught securely and are only authorised people given access to the images?
10. Do you evaluate your system regularly to make sure it is still required and could there be an alternative solution to a surveillance camera system?
11. Can the criminal justice system use the images and information produced by your surveillance camera system and do you have a policy on data storage, security and deletion?
12. Do you use any specialist technology such as ANPR, AFR, BWV or remotely operated vehicles (Drones) and if so do you have a policy in place to ensure that the information contained on your database is accurate and up to date?

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

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.

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.

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)

DRAFT South Wales Police Privacy Impact Assessment

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. It is not unlawful, disproportionate etc per se but some might be concerned that in doing so you breach their privacy.**

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

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

The collection of personal information is via two CCTV cameras connected to the standalone laptop/server. The system 'extracts' a face from CCTV footage and then compares it against a pre-defined watch list. In doing so, the system does not save the live CCTV feed, only the matched face. The CCTV feed will of course be itself saved and that data management covered under a separate PIA.

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

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 and will be reviewed regularly to ensure accuracy and currency and will be deleted at the conclusion of the respective deployment.

AFR Identify

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.)

Custody nominal images will be loaded into application and will form the candidate list.

Probe images will be copied into the application along with candidate images.

The system will record when a probe image is compared against the candidate images, the search will be available within the audit log.

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

DRAFT South Wales Police Privacy Impact Assessment

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 PIA process.

A number of stakeholders have been consulted 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 PIA 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. Home Office Centre of Applied Science & Technology (CAST) – 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.

DRAFT South Wales Police Privacy Impact Assessment

Consultation has taken place after the initial phase of the project deployment to allow the upload of custody images onto a standalone laptop. Further Consultation is to take place prior to AFR Identify IT infrastructure and application integration.

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

AFR Locate

The operational imperative to deploy the technique as part of the control strategy for a high risk, high profile event has limited the opportunity for public consultation at this stage. However, use of this option 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.

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 PIA to ensure protection afforded to processing data secured by this technology.

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 LIO's is underway.

Data Protection Act Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- a) at least one of the conditions in Schedule 2 is met, and**
- b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**

DRAFT South Wales Police Privacy Impact Assessment

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?	The conditions will be the engagement of technology to assist in the identifications of individuals in order to prevent or detect crime. Police and Criminal Evidence Act engaged for AFR Identify.
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?	Please see the above entry as there is no intention to rely on consent.
1.7 What information is collected, used, disseminated, or maintained in the system?	Watchlist information will realise matches to systems and databases to include false positives, the operator details and an audit log. Custody nominal images and probe images (to include Nominal naming convention.)

DRAFT South Wales Police Privacy Impact Assessment

<p>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?</p>	<p>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.</p>
<p>1.9 Is there a specific business purpose that requires the use of this information?</p>	<p>Policing purposes generally – in assisting in the location and identification of individuals. AFR Locate will assist in SWP becoming more efficient and effective in identifying 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.</p>
<p>1.10 Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?</p>	<p>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 is operational use, the system will be securely stored.</p>
<p><u>1.11 Human Rights Act:</u> 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?</p>	<p>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 or the prevention of crime allow. As the system progresses, CCTV feeds will only take place from public areas so no collateral intrusions into wider private lives is anticipated. Custody nominal images will be used to form the candidate list.</p>

Principle 2:

DRAFT South Wales Police Privacy Impact Assessment

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

<p>2.1 What are the main uses of the information? Does your project plan cover all of the purposes for processing personal data?</p>	<p>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.</p> <p>AFR Locate will involve enrolling images of known and unknown individuals into a watch list 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.</p> <p>AFR Identify will be used to compare digital images both still and moving against SWP custody database in order to identify them.</p>
<p>2.2 Have you identified potential new purposes as the scope of the project expands?</p>	<p>Yes, early considerations suggest that use of the product will diversify as the relationship with it matures. Proof of concept will be followed by integration of AFR 'locate' 'identify' within stand-alone and fully integrated systems.</p> <p>Future developments can potentially look at interfaces with other databases such as PND, ANPR, Passports, and DVLA.</p>
<p>2.3 Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?</p>	<p>Mitigation from the outset was secured by the provision of a non-networked solution, thereby eliminating any web application vulnerabilities. Operators will work in tandem and never alone with some early product also filmed to support academic evaluation.</p> <p>An operator cannot access any stored data, only another with 'administrator' level access to evaluate and prevent deletion control.</p> <p>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.</p> <p>Data transfer issues have already been dealt with and retention will be compliant with MOPI requirements.</p>

DRAFT South Wales Police Privacy Impact Assessment

	Intervention teams will be in possession of an application that secures data onto a receiving device.
Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are 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 purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	
5.1 What retention periods are suitable for the personal data you will be processing?	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. Separate to this requirement, an application will be made to retain an academic pool of data for a longer period – but for no more than is absolutely necessary - arguably justified

DRAFT South Wales Police Privacy Impact Assessment	
	to ensure a consistent dataset and a more level reporting field – set against the need to repeat exercises over and over to realise the same product.
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.
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.
Principle 6	
Personal data shall be processed in accordance with the rights of data subjects under this Act.	
6.1 Will the systems you are putting in place allow you to respond to subject access requests more easily?	No, because we are not retaining the data relating to personal information by name – therefore a FOI request or Subject Access Request will fail as we will not be able to identify the person from the data stored by name – just an anonymous image. 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 7	
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	
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.

DRAFT South Wales Police Privacy Impact Assessment

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 CAST 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.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

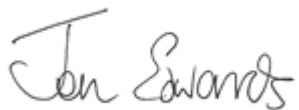
DRAFT South Wales Police Privacy Impact Assessment	
8.1 Will the project require you to transfer data outside of the EEA?	No. Some data will be cloud based (evidence.com) a data centre located in the UK
8.2 If you will be making transfers, how will you ensure that the data is adequately protected?	Technically 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.
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 CAST 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 CAST. Enquiries will determine whether a PIA 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	A service level agreement already exists with UPSI over the handling of personal data for the purposes of academic evaluation of policing matters.

DRAFT South Wales Police Privacy Impact Assessment

in a data-sharing agreement? If so, please describe.	
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?	All staff are vetted.
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?	No
11.2 Do individuals have an opportunity to consent to particular uses of the information, and how?	No
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.
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

DRAFT South Wales Police Privacy Impact Assessment		
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.	
Signature of person completing the PIA	Date:	12th February 2018
	Name (in capitals)	SCOTT LLOYD Inspector
Approval Signature (Approval will be required by either the Senior Responsible Officer (SRO)/ the Information Asset Owner (IAO) or Head of Unit (HoU))	Date:	

DRAFT South Wales Police Privacy Impact Assessment



Name (in capitals)

**Jonathan Edwards
T/ASSISTANT CHIEF CONSTABLE**

Guidance notes on these questions can be found in the PIA Code of Practice available from the ICO website:

<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>