Automated Facial Recognition

Guiding principles for Artificial Intelligence and the ethical use of Automated Facial Recognition

ASIAL
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED

Background

The Australian Security Industry Association Limited (ASIAL) is the peak body for security professionals in Australia. Our members include leading companies offering products and services that incorporate Automated Facial Recognition (AFR) technology for authentication, security, and public safety applications.

Automated Facial Recognition (AFR) is a technology capable of matching a human face from a digital image or a video frame against a database of faces. It has been designed to improve the safety and wellbeing of people, as well as providing a tool to assist and speed up operational processes, typically being used to authenticate users through ID verification services and works by pinpointing and measuring facial features from a given image.

AFR is one of many data analysis technologies which sit under the overarching umbrella of Artificial Intelligence (AI), a branch of Computer Science.

The ethics of AI and its application need to be regularly reviewed to ensure that it is not allowed to act autonomously without human oversight and it should not be used in any way which causes harm to individuals.

To provide guidance for the ethical use of AFR technologies, ASIAL has prepared a guidance document.

Acknowledgment

ASIAL would like to acknowledge the work of the British Security Industry Association whose guidance document on the use of AFR (*Automated Facial Recognition - A guide to ethical and legal use*, British Security Industry Association, 2021) contributed substantially to preparation of this document.

Introduction

There is no single global ethical framework for the safe use of AI. However, the Organisation for Economic Cooperation and Development (OECD) recommendations identify five complementary values-based principles for the responsible stewardship of trustworthy AI:

- AI should benefit people and the planet by driving inclusive growth, sustainable development, and wellbeing.
- AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards, e.g. enabling human intervention where necessary to ensure a fair and just society.
- There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.
- AI systems must function in a robust, secure, and safe way throughout their life cycles and potential risks should be continually assessed and managed.
- Organisations and individuals developing, deploying, or operating AI systems should be held accountable for their proper functioning in line with the above principles.

AFR is one of many different types of AI technologies, using machine learning algorithms to analyse and identify patterns in facial features from images or videos enabling the system to recognise and differentiate between individuals. Users should provide an overall AI plan covering the governance of Artificial Intelligence across the organisation which incorporates Automated Facial Recognition (AFR). The applications for AI span across multiple sectors from government, defence, healthcare, hospitality through to manufacturing, transport, and retail.

How is AFR used?

AFR is used in different scenarios by a wide range of organisations across multiple sectors. It is capable of finding a face in an image and mapping the features to create a pattern. This pattern can then be matched against other images that are stored within a database to either verify a high level of likeness (e.g. check against a passport photo; controlled environment), or identify as being present in a specific location at a particular time (e.g. a person of interest at a public event - dynamic environment) if their image is held in a general database.

Once the verification or identification process has taken place, the authentication is then confirmed by either the AFR technology or passed to a human to make the decision (to confirm the recognition and either action or do nothing), which process is dependent on the specific scenario and operational requirements.

Generally, AFR technology confirms authentication where the data has been supplied with express or implied consent and is being actioned within a controlled environment. In contrast, a human confirms authentication for mass surveillance where the subject is not necessarily aware of observation or where AFR is deployed within a dynamic environment.

Ethical considerations for specific use of AFR

Humans have long relied on the unique characteristics of the face to identify each other. With facial recognition systems evolving and maturing, they now offer unprecedented opportunities to automate and enhance this age-old practice faster, more accurately and reliably than the human eye.

Whilst many of us are comfortable with using our face to unlock a smartphone, there are significant concerns about the use of AFR in areas such as public surveillance and law enforcement. Ethical concerns related to facial recognition such as racial bias, privacy, lack of informed consent and transparency, mass surveillance and data breaches are important issues that need to be addressed.

ASIAL is committed to a responsible and ethical approach to the use of AFR in compliance with all applicable regulations and laws.

Core Principles for the ethical use of AFR

1. Transparency

Transparency is the foundation that underpins the use of AFR for both public and private use. AFR should be used transparently to enable the person to provide consent to the use of their personal data.

The use of AFR should be proportionate to the purpose i.e. the problem being solved. It should be clear when and for what purpose the technology is being used, along with processes and procedures covering collection, processing, storage, use and transfer of related data. There must be a lawful basis for processing personal data and it should be considered whether the same objective can be achieved by other less intrusive measures.

Users should provide public notice and secure consent when deploying AFR.

2. Non discrimination

AFR should not cause harm to any individual, with harm meaning a negative impact on privacy, dignity and human rights.

Facial recognition should only be used in ways and for purposes that are non-discriminatory. The technology within AFR cannot be inherently biased. It is how it is trained and how it is used which determines how accurate it may be in detecting features from the widest demographic in a range of lighting scenarios.

Inaccurate decisions that may be perceived as bias in the AFR system, for example difficulty in recognising faces from a diverse demographic, should be reported to the AFR provider who in turn should take immediate corrective action.

If there is an adverse impact on individuals who are not recognised, an alternative method of authentication should be considered.
AFR vendors shall periodically audit their technology to find areas where bias may have crept into the model and upgrade appropriately.

3. Clear and defined purpose

The use of AFR must clearly identify the purpose for use of the technology, the capabilities and limitations of the system and ensure that the chosen technology is correctly configured.

When using AFR, the necessary risk assessment and Data Protection Impact Assessment (DPIA) should be undertaken.

4. Accountability

Although AFR software automates image comparison and matching, it must not automate decision making without appropriate human oversight at a level commensurate with the application.

Instances where AFR could have a negative impact on the individual should result in the authentication process being confirmed by a human.

5. Data security

Data transmission, storage and processing should be optimised to ensure privacy and security through encryption, cybersecurity and privacy best practices.

Personal data should be obtained lawfully and within overarching ethical and legal guidelines. The database of images against which the AFR matches faces must be legally controlled as set in the Privacy Act 1988 (Cth) the principal piece of Australian legislation protecting the handling of personal information about individuals. It should be possible for an individual to find out if they are on a watch list through subject access requests or other legal means. It must be clear to the individual that they are giving consent by using an area controlled using AFR. Consider using automatic face obscuration/pixelation for live monitoring.
AFR systems shall have data retention periods defined and regularly delete data that is no longer required,

6. Privacy

AFR systems should be designed to comply with current and emerging data privacy laws, as well as supporting privacy practices and ongoing system maintenance.

There should be a strong culture of accountability internally and across third party providers and users of AFR, including development and disclosure of governance policies to enable an opportunity for feedback.

7. Training

Ongoing training must be provided to ensure users of AFR understand how to configure, maintain and operate the technology in line with their policies.

Providers of AFR technology should provide users, installers and operators with ongoing training to ensure deliver the most accurate and non-biased results.

How to apply this guidance

This guidance provides recommendations on the ethical use of AFR technology for beneficial use in both public and private sector environments to ensure it does not cause harm or discriminate against persons. It takes into account current known legislation, standards and guidance around AI and in particular AFR.

It is intended to be useful to system designers, installers/integrators and end-users.

This guidance does not cover the technical elements of AFR technology.

Assessing the need for AFR

There are important early-stage decisions which need to be made before the AFR is deployed taking into account the following steps:

- Define why AFR is needed.
- Define where AFR will be used.
- Define the purpose of its use, including key performance indicators.
- Undertake an ethical assessment based on legislative and consumer data protection guidelines.
- Undertake a DPIA and ensure ethical and legal compliance and proportionality.

If the location and purpose of the AFR is legal, ethical, and proportionate, you are ready to create an operational requirements specification.

Governance & compliance

Accountability

- Ensure an individual or group is nominated and held accountable for the ethical and legal compliance and operation of the system.
- Ensure there is an ethical and lawful basis for processing (e.g. consent/legitimate interest).
- Ensure the integrity of the data is protected based on the risk of processing.

Responsibility

- Ensure individuals and processing systems have defined and documented responsibilities and appropriate authorisation levels.
- Ensure policies are shared with and approved at strategic and/or board level.
- Ensure all processing activities are defined and documented.

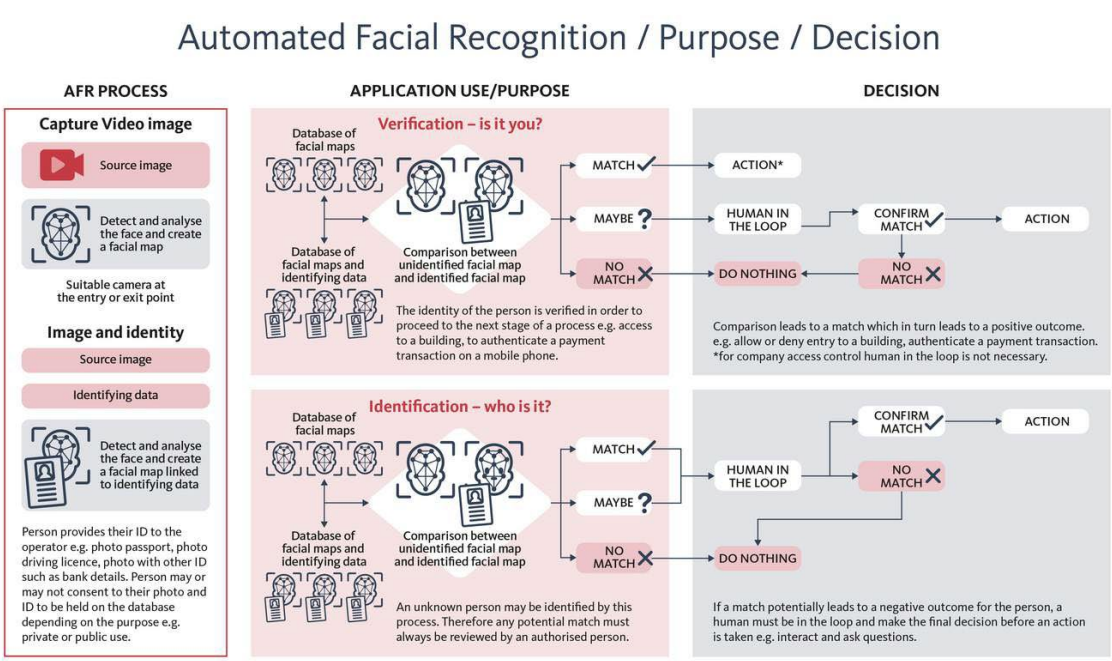
Privacy & Data Protection

- Ensure appropriate privacy data is made available for subject access requests.
- Ensure all data collected is necessary, proportionate, and stored for an appropriate amount of time and in a transparent manner.
- Ensure a suitable data protection policy is available and published as appropriate.
- Ensure there is a DPIA.

Operational requirement

The use of biometric technology such as face, voice and fingerprint recognition are becoming a part of our everyday lives; many personal devices such as mobile phones and computers use these technologies to provide greater privacy, security, and ease of use to access them, and in the same way, such technology is often used to control access (the right to passage) in the private sector business space. But with this technology comes a greater need to ensure those that are impacted by it are made aware of its purpose and that any personal 'data' captured will be used in an ethical way.

AFR systems can be split into two application use themes: for verification purposes (e.g. providing access) or for identification purposes (e.g. law enforcement). These can be depicted by the following process management summary:



Source: Automated Facial Recognition: A guide to ethical and legal use, British Security Industry Association, 2021

The three key elements of the process management are:

1. **Capture:** images from individuals are captured by the AFR system and presented to the reference databases to determine any further response.
2. **Application use/purpose:** dependent on the use of the AFR system, comparison takes place against a database to compare a potential match. Further detail on Verification and Identification applications are explained on pages 9 & 10.
3. **Decision:** this is the process of deciding whether a face is authenticated by a human for further action or disregarded/deleted.

Data privacy

Where AFR systems are to be considered, a DPIA must be carried out to determine the following:

- Identify the need for a DPIA (what the system aims to achieve/type of processing involved)
- Describe the processing (collect, use, share, store or delete data)
- Consultation process (how / when to obtain individuals views if/where appropriate)
- Assess necessity and proportionality (lawful basis for processing, can the same objective be
- achieved by other less intrusive measures?)
- Identify and assess risks (risk of harm to the individual)
- Identify measures to reduce risks (mitigation measures to be used)
- Confirm completion of the DPIA and record outcomes
- Integrate outcomes into the Operational Requirement
- Keep under review (review the purpose and need regularly)
- Ensure that appropriate signage is in place which warns the public on the use of AFR Video Surveillance Systems (VSS)
- Privacy masking/differential privacy should be utilised when appropriate.
- The data controller should be defined

Storage & retention

- Consider how long the data is to be kept/retained.
- Set out how often the data is to be reviewed.
- Data that is no longer needed must be erased and/or anonymised.
- The data should be stored securely through physical and electronic security measures.
- Data sharing agreements should be in place as appropriate, e.g. between an AFR.
- service provider and a subscriber/user.

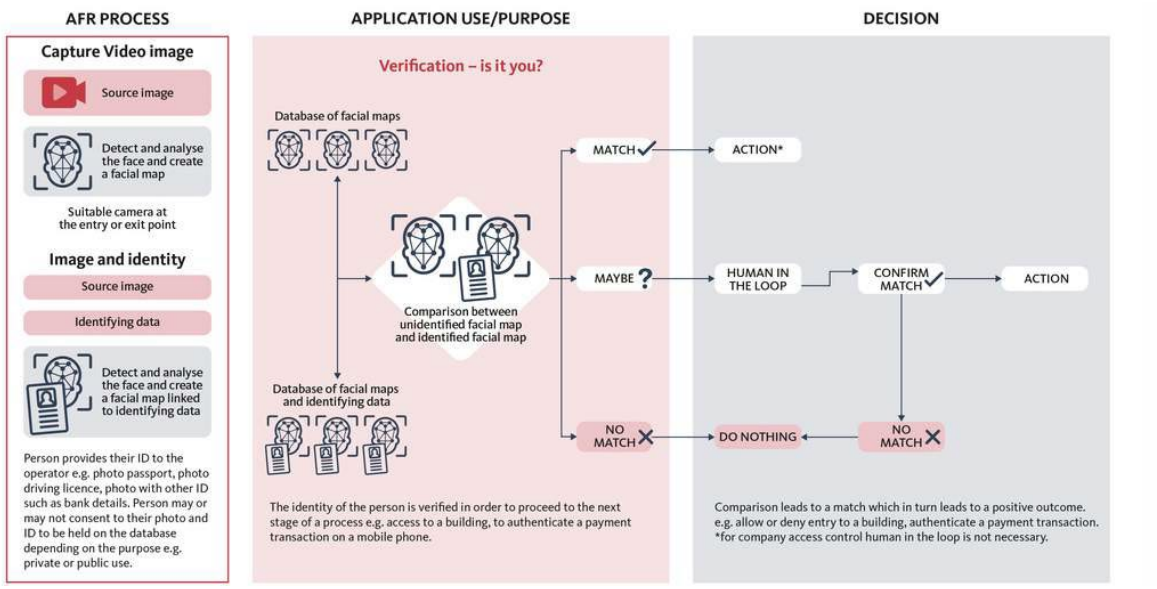
Reference database

- Define the purpose of the database in line with ethical and legal requirements.
- Define the process required for checking the contents of the database, e.g. deleting poor quality images/replacing with improved quality images, set a retention period. period/review of interested persons and review risk criteria.
- Where will the database be physically held and is it secure?
- Ensure that cyber security protections are in place to protect the data.
- Ensure that subject access requests, response times and publication of method to access.
- Consider if images need to be used for evidential purposes, e.g. data validation, image.

Verification - is it you?

The use of AFR is divided into two areas: for the purpose of verification, “is it you?” and for the purpose of identification, “who is it?”.

Where AFR technology is deployed in an organisation for verification purposes, it is important that policies are developed (or existing ones updated) to cover the explanations, considerations and actions that the organisation requires of its employees. Typically, these should cover: what the rules are, why the rules are in place and who the rules apply to.



Source: Automated Facial Recognition: A guide to ethical and legal use, British Security Industry Association, 2021

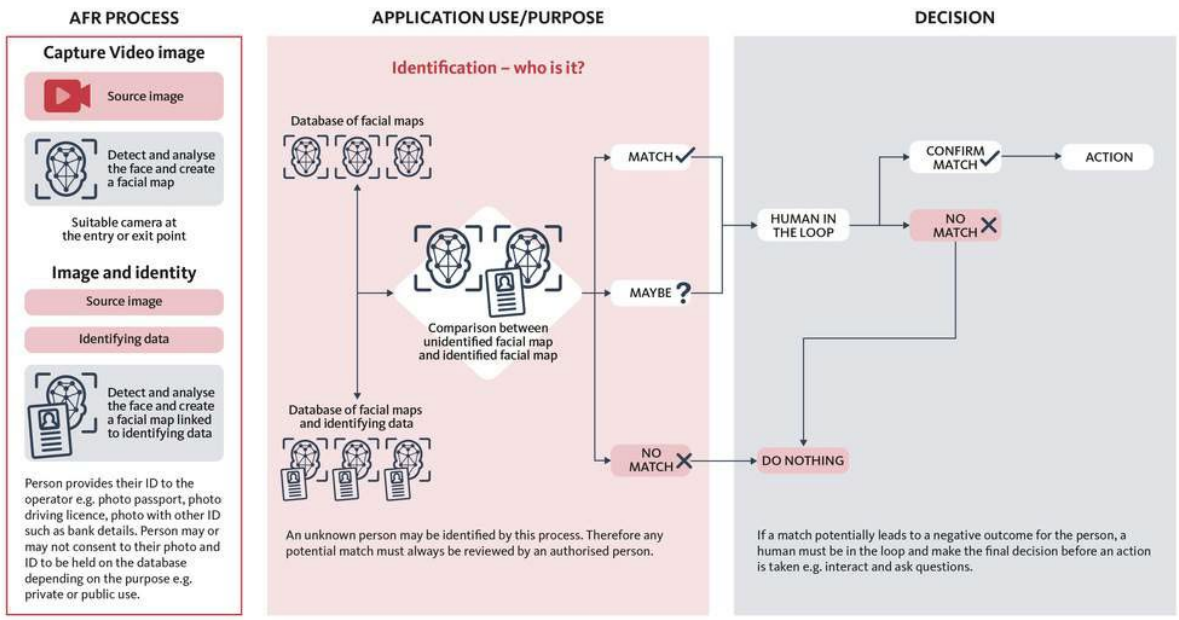
Typical cases for verification

- To manage/control the flow of individuals/queuing to meet business service levels and/or to gain authorised access to secure areas.
- Time and attendance applications to monitor persons of interest for the purposes of payroll and safety purposes i.e. fire evacuation safety, time spent in a specific area, repeat entering of a protected area.
- Personal access to mobile phones, computers, online banking.
- Border control/passports to allow the safe and valid passage of persons entering or leaving the country

Identification - who is it?

Where AFR technology is used for identification purposes such as by Law Enforcement* and other agencies, policies and procedures may take a different form as it may not be appropriate to consult widely with the persons of interest. That does not however mean that such organisations are exempt from the Privacy and Data Protection legislation. There will be a need to document persons of interest, whether they are likely to be present at a given time in a monitored location.

It is important that the software does not exhibit any form of bias towards any such persons. It should be made clear that AFR systems where data is stored privately (or by the Government) should be reviewed carefully to ensure they are lawful under Privacy legislation and if held in other locations are legal under the laws for that territory.



Source: Automated Facial Recognition: A guide to ethical and legal use, British Security Industry Association, 2021

Typical cases for identification

- Border control to identify persons on a known approved watchlist.
- For use in private venues by the owners - shops, museums, stadiums, leisure centres and other private venues where there is a need to control theft or anti-social behaviour.
- For law enforcement purposes to alert to the presence of individuals of interest.
- For private security companies - shopping centres, local authorities to alert to the presence of individuals of interest.
- For law enforcement purposes following VSS footage collected after a notable event or incident.
- Inclusion onto a watch list for the purpose of alerting other business owners of person of interest that may be under suspicion of having committed an offence.

References

The following documents provide helpful reference material.

- *Automated Facial Recognition - A guide to ethical and legal use*, British Security Industry Association, 2021
- Australian Privacy Policy https://www.oaic.gov.au/privacy/australian-privacy-principles
- From Light to Intelligent Pixels, by Vlado Damjanovski, ASIAL (2022)
- General Data Protection Regulation, www.gdpr-info.eu
- National Institute of Standards and technology - www.nist.gov/artificial-intelligence
- OECD Privacy Guidelines, www.oecd.org/digital/privacy
- *SIA Principles for the Responsible and Effective Use of Facial Recognition Technology*, Security Industry Association 2020
- Video surveillance systems for use in security applications – AS62676:4:2020