FACT SHEET – FACE MATCHING SERVICES

The Australian Government is working with states and territories to implement new biometric face matching services. These services have been developed to protect Australians from identity crime, and provide law enforcement and security agencies with a powerful new investigative tool to stay one step ahead of terrorists and criminals that seek to circumvent Australia’s identity checking processes.

On 5 October 2017, the Prime Minister and state and territory leaders signed an Intergovernmental Agreement on Identity Matching Services. Under the Agreement, agencies in all jurisdictions will be able to use new Face Matching Services to access passport, visa, citizenship, and driver licence images – while maintaining robust privacy safeguards.

The use of the Face Matching Services will:

- protect people from identity theft, and help victims restore their compromised identities
- prevent criminals and terrorists creating and using fraudulent identity documents
- assist police to investigate other serious criminal activity
- help people to prove who they are when using government services online.

Face Verification Service (FVS)

The FVS is a one-to-one image based verification service that can match a person’s photo against an image on one of their government records, such as a passport photo, to help verify their identity. Often these transactions will occur with the individual’s consent.

For example, where a person uses their citizenship record as evidence of their identity to apply for a passport, the system could enable the passport office to ask the Department of Immigration and Border Protection to confirm the identity of the passport applicant.

Face Identification Service (FIS)

The FIS is a one-to-many image based identification service that can match a photo of an unknown person against multiple government records to help establish their identity. Access to the FIS will be restricted to agencies with law enforcement or national security related functions.

Police will use the FIS for investigations of more serious offences. For example, it may be used to identify a suspected paedophile from child exploitation material, or to identify an armed robber from a still image taken from CCTV footage. It will not be used for minor offences such as littering or parking infringements, but it may be used to help identify victims of disasters and to locate missing persons.
Access to the FIS will only be provided to a limited number of users in specialist areas with training in how to interpret the results. It does not provide for fully automated or 'real time' surveillance of public spaces, but does enable more targeting searching using still images, taken from CCTV for example, to quickly identify a 'person of interest' for public safety purposes.

Why these services are necessary

The Australian Government is investing in this new system to help combat identity crime, which is one of the most common crimes in Australia and costs around $2.2 billion per year. Around 1 in 20 Australians experience identity crime each year that results in financial loss.

Identity crime is a key enabler of serious and organised crime, such as drug trafficking, money laundering, people smuggling, child exploitation and terrorism. Australians convicted of terrorism offences have used false names to avoid detection while planning attacks. This includes purchasing ammunition and chemicals to make explosives and pre-paid mobile phones to communicate anonymously.

An operation by the joint Australian Federal Police and New South Wales Police Identity Security Strike Team found that around 1,700 fraudulent identities seized from just one criminal syndicate were linked to:

- 29 high profile criminals linked to historic or ongoing drug investigations
- more than $7 million in fraud against individuals and financial institutions, and
- more than $50 million that was laundered offshore and was likely to be proceeds of crime.

While existing measures such as the Document Verification Service (DVS) are helping to prevent the use of fake identity documents, criminals are now producing high quality fraudulent identity documents. These false documents contain personal information stolen from innocent and unknowing victims, but with someone else’s photo – documents that would pass a DVS check. Preventing this type of fraud can be assisted by greater use of biometrics, such as the FVS and FIS.

How the system works

The Face Matching Services draw on existing collections of images that are used by government agencies for issuing evidence of identity documents. But there is no single database that will hold all passport, visa, citizenship and driver licence images.

A central Hub or exchange facilitates data sharing between agencies on a query and response basis, without storing any personal information. This enables better auditing and oversight, while maintaining data sources separately.

Passport, visa and citizenship images will continue to be held by the Commonwealth agencies that issue these documents, and that already have facial recognition systems.

Driver licence images will be made available via a common facial recognition system, hosted by the Commonwealth on behalf of participating state and territory driver licencing agencies.

This is the most cost effective way of providing access to these images as not all states and territories currently use facial recognition for their driver licence images – which can leave them more susceptible to fraud. The system will provide additional face matching services for states and territories to help improve the integrity of driver licence data holdings.
Data contributed by the states and territories will remain under their control. The Commonwealth will not have direct access to this information - access will only be provided in accordance with data sharing agreements with the states and territories.

**Why legislation is needed**

A range of legislation already authorises the sharing of facial images for law enforcement purposes and other purposes.

New Commonwealth legislation is needed to authorise the collection, use and disclosure of driver licence information via the central driver licence database. This legislation will not increase the powers of police agencies to collect this information, or to use information in ways that they are not already authorised to do. It will provide a more transparent basis for the Commonwealth to operate the driver licence database, with additional privacy safeguards.

**Security and privacy protections**

The system will adopt best practice security and access arrangements in accordance with the Government’s Protective Security Policy Framework and the Information Security Manual, and will be subjected to independent penetration and vulnerability tests as well as an independent security review by the Australian Signals Directorate.

The central infrastructure will exchange messages but it will not conduct any matching nor store any personal information. This approach allows individual agencies to retain full control over their own image holdings and decisions about the organisations with which they share this information.

The driver licence component of the system will be hosted separately and remain under the control of participating states and territories. The Commonwealth will not have direct access to this information - access will only be provided in accordance with data sharing agreements with the states and territories.

Participating agencies will require a lawful basis to collect and use facial images, just as they do now.

The system will have robust privacy safeguards, informed by independent privacy impact assessments conducted throughout the design and implementation phases, in consultation with the Australian Privacy Commissioner. These assessments will be published wherever possible, so that the community can see the safeguards that are being built into the system.

Participating agencies will need to enter formal data sharing agreements containing safeguards for the sharing and use of personal information, and regular audits will help ensure that these protections are functioning properly. Agencies will continue to be subject to independent oversight by a range of existing external bodies such as privacy commissioners, ombudsmen and anti-corruption or integrity commissioners for their use of personal information. The operation of the system will be audited by the Office of the Australian Information Commissioner.

For more information contact the Attorney-General’s Department at identity.security@ag.gov.au