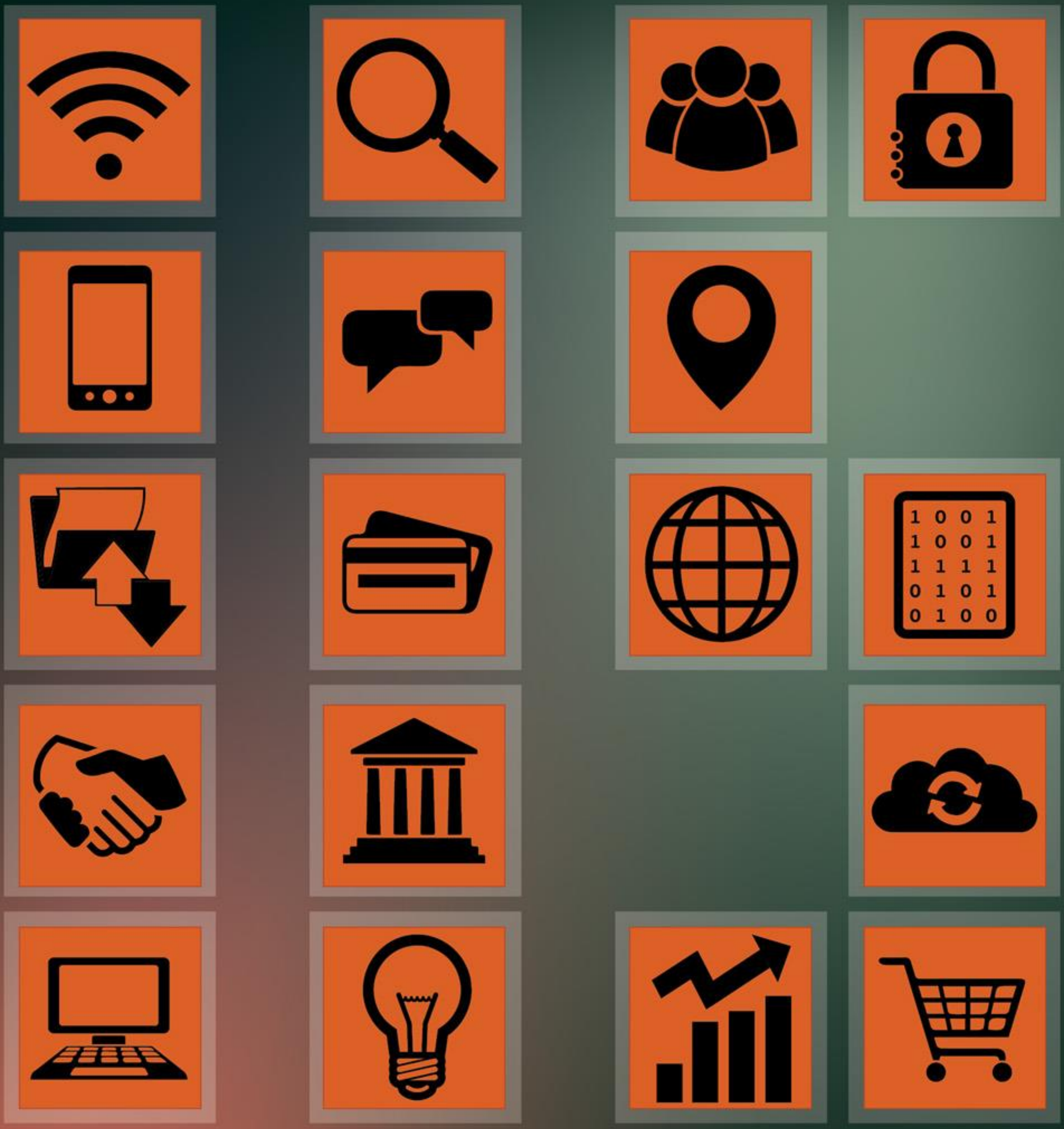


National Driver Licence Facial Recognition Solution Privacy Impact Assessment Report

Commercial-in-Confidence

For: Attorney-General's Department

Date: November 2017

INFORMATION
INTEGRITY
SOLUTIONS

managing the **privacy** of **individuals** is **complex** and we can help you get it **right**

Table of Contents

Glossary

Abbreviation or term	Expansion or definition
APPs	Australian Privacy Principles
FIS	Face Identification Services
FMS AB	Face Matching Services Advisory Board
FOI Act	*Freedom of Information Act 1982 (Cth)*
FRAUS	Facial Recognition Analysis Utility Service
FVS	Face Verification Services
COAG	Council of Australian Governments
Hub	Interoperability Hub
MCPEM	Ministerial Council for Police and Emergency Management
NDLFRS	National Driver Licence Facial Recognition Solution
NFBMC	The National Facial Biometric Matching Capability
NISCG	National Identity Security Coordination Group
OAIC	Office of the Australian Information Commissioner
OPOLS	One Person Once Licence Service
Privacy Act	*Privacy Act 1988 (Cth)*
RTA	State and Territory Road Transport Agencies

1. Executive Summary

The Attorney-General's Department (AGD) engaged Information Integrity Solutions Pty Ltd (IIS) to undertake a privacy impact assessment (PIA) of the proposed design, operation and governance of the National Driver Licence Facial Recognition Solution (NDLFRS). The NDLFRS is part of the National Facial Biometric Matching Capability (NFBMC).

The NFBMC is intended to improve detection and prevention of fraudulent identities to support national security, law enforcement, community safety and service delivery, while maintaining robust privacy safeguards. It comprises the Interoperability Hub (Hub) which transmits matching requests and responses between authorised agencies and organisations via defined Face Matching Services, the NDLFRS to help make available driver licence images via these Face Matching Services, the legislative framework within which these systems operate along with training and other related standards to support greater integrity and consistency in data sharing across jurisdictions.

The Face Matching Services that are provided through the NFBMC enable agencies (Requesting Agencies) to compare a facial image against databases of facial images held by other agencies (Data Holding Agencies) to help verify the identity of a known individual, identify an unknown individual or detect individuals with multiple fraudulent identities.

The NDLFRS is the technical solution by which Road Transport Agencies (RTAs) participate in the NFBMC, enabling the sharing and matching of driver licence images amongst RTAs, and between RTAs and other agencies consistent with legislative permissions and interagency data sharing agreements.

AGD is aware of the potential privacy risks in the use of biometric matching processes and is aiming to build in robust privacy safeguards to offset the risks as the NFBMC, including the NDLFRS, is implemented. It has committed to using Privacy by Design (PbD) approaches and has commissioned a number of PIAs, including this one, to inform the development of the NFBMC and the NDLFRS solution design, operations and governance.

1.1 NDLFRS overview including bodies involved

AGD would host the NDLFRS that involves establishing:

- A combined (but partitioned) store of replicated driver licence facial images, biographic and related driver licence information from each of the state and territory RTAs
- A shared facial matching engine that would ensure all RTAs can access highly capable facial recognition and matching technology for use on their own images.
- An architecture that renders driver licence facial biometric data searchable for matching purposes on a national basis via the NFBMC's Face Matching Services, whilst retaining control over the sharing of that data with the states and territories, and respecting privacy rules.

The Face Matching Services that would use NDLFRS data (via the NFBMC Hub) are:

- The Face Verification Service where matches are conducted on a one-to-one basis for each data source that is queried to verify that two separate images are of the same person
- The Face Identification Service where matches are conducted on a one-to-many basis for each data source that is queried to determine the identity of an unknown person, or detect instances where someone has multiple potentially fraudulent identities
- The One Person One Licence Service that enables RTAs to conduct a narrowly focused check, on a constrained one-to-many basis, to identify any multiple licence holdings in the same or different identities across participating jurisdictions
- The Facial Recognition Analysis Utility Service that would provide RTAs with access to facial matching technology, for use on their own data within the NDLFRS, via facial recognition tools made available within their own local system infrastructure

A range of Commonwealth, State and Territory agencies and private sector organisations (participating bodies) will be permitted to share facial images and related biographic data via the Face Matching Services for approved purposes (law enforcement and national security, protective security, community safety, road safety and service delivery), provided they have a lawful basis, meet the policy and procedure requirements and sign formal data sharing agreements.

IIS' overall opinion

IIS finds that the inherent privacy risks for the NDLFRS are high. Central to this assessment are the facts that:

- Biometric information, such as a facial image, is considered intrinsically sensitive and is treated so in the Privacy Act (although not necessarily in privacy laws in other jurisdictions)[1]
- Driver licence photographs are also subject to special use and disclosure rules under state and territory road transport laws and regulations
- The NDLFRS would replicate and centralise extremely large, existing data holdings of facial images for face matching using facial recognition technologies
- AGD would be a facial recognition services provider to RTAs as well as a provider of Face Matching Services to all participating agencies
- The images would be used for purposes beyond the initial purpose of collection.

[1] Privacy Act, s.6(1) definition of sensitive information
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html

IIS's privacy assessment has also identified a number of privacy risks that could arise from the system's operation and governance. The key risk areas identified are:

- The transparency measures to inform individuals or the community about transfers of information from RTAs to AGD for use in Face Matching Services and about the NFBMC as a whole
- Security risks as information is transferred to the NDLFRS and as the system is used by RTAs or other agencies
- Data inaccuracy or face matching errors leading to inconvenience or harm to individuals
- The multi-agency and multi-jurisdictional nature of the NFBMC, including the NDLFRS, making effective privacy oversight challenging and/or making it difficult for individuals to resolve privacy issues
- The potential for function creep – that is for the driver licence data to be used for additional unexpected new purposes or for the system to expand in ways not currently envisaged at the time of the preparation of this PIA.

In IIS' view AGD is giving serious consideration to the privacy risks emerging at this stage in the development of the NDLFRS. IIS considers that most of the risks identified are likely to be managed via the complementary set of strong privacy and security controls that AGD is proposing. IIS has nevertheless made recommendations to strengthen the protections in a number of areas.

The wider question of the privacy impacts associated with participating agencies using the Face Matching Services against data held in the NDLFRS, or by RTAs for driver licence issuance or other data management activities is outside the scope of this PIA. IIS considers this to be a limitation on this privacy impact assessment that needs to be considered very carefully.

IIS recognises and welcomes the fact that AGD would be commissioning further PIAs as the system develops and that it is requiring participating agencies to also undertake their own PIAs that examine the proposed uses of the Face Matching Services. IIS also acknowledges that AGD intends to undertake a final whole of system PIA once the NFBMC, including the NDLFRS, is fully implemented and all current services are operational.

However the incremental approach could mean that the privacy impacts of the system as a whole are not sufficiently considered. This could mean that the opportunity to identify and manage potentially significant risks created by the system as a whole is lost.

1.2 Recommendations

IIS has made 18 recommendations that are outlined in full in the table in Appendix A. The recommendations cover the following matters:

- NDLFRS operations:
  - Ensuring RTAs control NDLFRS information and ensuring individual rights are maintained
  - Transparency and information for individuals
  - Requirements for consent based access to NDLFRS

  - Process to handle false negative matches
  - Monitoring data accuracy and matching processes
  - Formal data retention policy
  - Clarity on roles and processes in responding to requests for access to information
  - Proactive and coordinated data breach management
  - Benefits realisation.
- NDLFRS governance:
  - Governance body membership
  - Publication of privacy impact assessments for the NDLFRS access
  - Annual reports on use of NDLFRS for Face Matching Services and OPOLS
  - OPOLS Access Policy
  - NISCG policy and guidance on audits
  - Seamless privacy oversight and investigations
  - Review of the operation of the NDLFRS
  - Gaps in privacy safeguards where jurisdictions do not have privacy law
  - Changes to the NDLFRS.

2. Introduction

The Attorney-General's Department (AGD) engaged Integrity Solutions Pty Ltd (IIS) to undertake a privacy impact assessment (PIA) of the proposed National Driver Licence Face Recognition Solution (NDLFRS).

The NDLFRS would bring together driver licence images, biographic information (name, date of birth, gender) and related information about the licence (address, licence number, currency, conditions etc.) from each of the states and territories, in a system hosted by the Commonwealth. Specified subsets of this information would be made available via the various Face Matching Services provided by the National Facial Biometric Matching Capability (NFBMC).[2]

The inclusion of a centralised source of driver licence images was always within scope of the NFBMC (although this was initially proposed to be hosted by Austroads on behalf of the states and territories). It is nevertheless a significant expansion beyond the initial implementation of the NFBMC amongst Commonwealth agencies. It would facilitate access to images of most adult Australians via the Face Matching Services. In line with its commitment to privacy by design (PbD) AGD is seeking an assessment of privacy risks to inform the NDLFRS solution design, operations and governance.

2.1 Scope of the PIA

AGD asked IIS to assess the NDLFRS focussing on:

- The design of the NDLFRS, including the architecture, data replication and security protocols
- The proposed operating model, including:
  - How the system would technically implement or service the face matching requests between RTAs, and between RTAs and other agencies, via the NFBMC
  - AGD's role and responsibilities in hosting and managing the system on behalf of the states and territories
  - The responsibilities and obligations for RTAs, including in relation to maintaining accuracy of data, providing notification to its users, and responding to public inquiries
  - The proposed governance arrangements, including participation of state and territory data owners and consumers within the different governance bodies.

IIS was not asked to assess the privacy impacts associated with the sharing of images and biographic and related driver licence information from the NDLFRS between RTAs, or with other participating agencies, via the Hub. These information flows would be the subject of further separate PIAs.

[2] See Appendix D for information flows for each of the face matching services

For most states and territories participation in the NDLFRS would require legislative amendments to remove restrictions on the sharing of driver licence images with the Commonwealth. The Commonwealth is also proposing to introduce legislation to facilitate the NFBMC programme, including its hosting of the NDLFRS, which may assist in removing restrictions for some states or territories. This legislation is subject to a separate PIA and is not within scope of this PIA.

The methodology for this PIA, including meetings held and documents reviewed, is at Appendix B.

3. NDLFRS overview

3.1 The NFBMC and Interoperability Hub

All Australian Governments have committed to collaborative action to promote the right of Australians to a secure and protected identity through the National Identity Security Strategy, which was endorsed by the Council of Australian Governments (COAG) in 2007 and again in 2012. One of the strategy's goals is to promote the interoperability of biometric identity management systems.

The Commonwealth, through AGD, has been leading the development of the NFBMC to take forward the National Identity Security Strategy and support related law enforcement, national security and service delivery objectives. The NFBMC provides facial biometric matching services, including a Face Verification Service (FVS) and a Face Identification Service (FIS) against holdings of facial images, amongst Commonwealth agencies, and between the Commonwealth and states and territories.

The Face Matching Services are or will be facilitated and controlled via the Biometric Interoperability Hub (the Hub). The Hub commenced operations in October 2016. The first phases of the NFBMC involved establishing the FVS (one-to-one matching) for visa, citizenship and passport images, which is now complete. The FIS (one-to-many matching) against visa and citizenship images is due to commence in early 2018 for an initial cohort of Commonwealth law enforcement users. The FIS against passport images will then follow in late 2018, rendering all of the Commonwealth's images available through the Face Matching Services.

The Hub does not collect or store any biometric, biographic or other personal information, nor does it perform any matching. The matching occurs within the Data Holding Agencies that operate their own facial matching technology (or in the case of RTAs, the NDLFRS). The Hub simply functions as an information broker, facilitating the secure, automated and auditable sharing of facial images between the participating agencies. Agencies using the Face Matching Services must have a lawful basis to collect, use and disclose facial images.

More information about the NFBMC, including IIS' preliminary PIA of the Hub, is available from AGD's website at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Face-verification-service.aspx.

3.2 The NDLFRS

Driver licences are the most commonly used photographic identity document in Australia and have been identified as critical data source for the NFBMC. AGD is now moving to make driver licence photos and related information available via Face Matching Services. Driver licence information is held by Road Transport Agencies (RTAs) in each of the state and territories.

The NDLFRS is the technical solution, hosted by the Commonwealth on behalf of the states and territories, to enable the sharing and matching of driver licence images amongst RTAs, and between RTAs and other agencies, via the Hub and the Face Matching Services.

The policy, legislative, financial and governance arrangements for state and territory participation in the NDLFRS and the NFBMC more broadly are set out in an *Intergovernmental Agreement on Identity Matching Services* (IGA) that was agreed by COAG in October 2017. A copy of that IGA is publicly available and can be accessed on the COAG website:
https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf

The NDLFRS is in the pilot and development phase. The underlying infrastructure has been purchased and configured (located in a secure data centre under contract to AGD). Technical teams are now in the detailed design and build phase, with pilot work complete or being undertaken with several RTAs (Northern Territory, Tasmania, Victoria, South Australia). The aim is for the NDLFRS to commence operation, with an initial tranche of participating jurisdictions, in mid-2018 with other jurisdictions to follow throughout 2018.

3.2.1 Matching services using the NDLFRS

The NDLFRS would support the following types of facial biometric matching functionality for agencies participating in the Face Matching Services provided by the NFBMC:

- FVS matches that are conducted on a one-to-one basis for each data source that is queried to verify that two separate images are of the same person. By only focusing on the matching of a single asserted identity, verification matches minimise privacy impacts and provide the potential for high transaction volumes and near real-time processing
    - The FVS would be made available to a broad range of government agencies, and potentially in future private sector organisations, to assist in verifying a person's identity.
- FIS matches that are conducted on a one-to-many basis for each data source that is queried. Identification matches can assist in detecting duplicate or fraudulent identity records, where images of the same person are linked to different names or other biographical information. Unlike FVS matches, identification matches require human involvement to review galleries of results from the matching process and perform the identity resolution task. As such, they cannot be fully automated with near real-time responses. There are also more risks in the process, including because of the potential for identity resolution specialists to make mistakes. The FIS would only be made available to agencies with law enforcement or national security related functions.

- One Person One Licence Service (OPOLS) enables the road agencies to conduct a narrowly focused check, on a constrained one-to-many basis, to identify any multiple licence holdings in the same or different identities across participating jurisdictions.

  A facial image, and claimed birth year plus and minus one/two years, would form the request parameters necessary to undertake such a query. The query would be generated locally from RTA back-end licencing systems and undertaken across some, or all, participating RTAs. The outcome of the match would be a return of the top two or three image matches from each queried jurisdiction, above a predetermined, very high match threshold. A nil response would indicate this person is not on any other state/territory databases at the time of the query being undertaken

  - The OPOLS would only be made available to RTAs or agencies that contribute data to the NDLFRS.

- Facial Recognition Analysis Utility Service (FRAUS) would provide RTAs with access to facial matching technology via facial recognition tools made available within their own local system infrastructure. RTAs would be positioned to undertake data integrity analysis of their own data holdings and remediation to the extent that makes sense within each jurisdiction, dependent on their own priorities and resources. Individual agencies may choose to undertake such analysis incrementally, for example by targeting analysis at higher risk segments of licence holdings

  - The FRAUS would only be made available for agencies to analyse their own data within the NDLFRS. (Access to the FRAUS is provided directly via the NDLFRS, unlike the other Face Matching Services above which are facilitated via the Hub as they involve data matching or sharing between different agencies).

3.3 NDLFRS Operating model

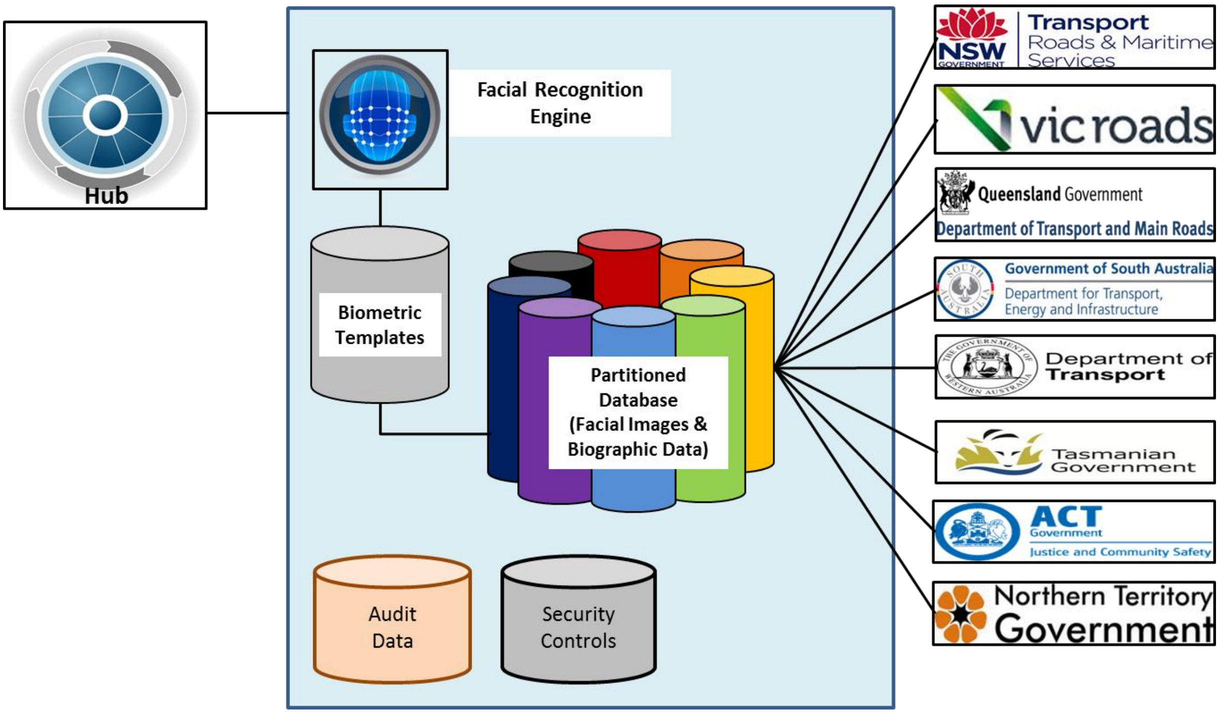
The proposed architecture of the NDLFRS involves a partitioned database(s) of driver licence images and biographic and related driver licence information, with each RTA replicating their records to, and maintaining direct control over, their own partition in the database. The images would then be enrolled in a common facial recognition engine to create biometric templates. These templates would be stored in a separate partitioned database to the raw images and biographic and related driver licence information.

As the host of the NDLFRS, the Commonwealth will not have any direct access to the images or biographic and related driver licence information held within the system and cannot alter this information. This information can only be accessed via the Face Matching Services, in accordance with arrangements that need to be agreed with the states and territories. Similarly, RTAs would not have access to the template database and cannot alter information within it.

Except in circumstances where an RTA is accessing its own data (e.g. the FRAUS), all matching requests against the NDLFRS would come via the central Hub to ensure the strict access controls are applied. Audit information is collected for every transaction.

The following diagram gives a high level overview of the NDLFRS architecture and shows how RTAs would interact with one another and with the external NFBMC Interoperability Hub to make available this set of services.

Figure 1 – High-level overview of the proposed NDLFRS architecture


Hub
Facial Recognition Engine
Biometric Templates
Partitioned Database (Facial Images & Biographic Data)
Audit Data
Security Controls
NSW Government Transport Roads & Maritime Services
vicroads
Queensland Government Department of Transport and Main Roads
Government of South Australia Department for Transport, Energy and Infrastructure
Department of Transport
Tasmanian Government
ACT Government Justice and Community Safety
Northern Territory Government

3.3.1 Personal information flows

3.3.1.1 Personal information held in NDLFRS

AGD is in the process of defining with RTAs the set of personal or sensitive information that would be included in the NDLFRS. A definition of 'identification information' that covers the data held in the NDLFRS will be included in proposed legislation to support the NFBMC. The legislative approach would mean that the NFBMC and NDLFRS operations would be more transparent.

Some RTAs have expressed an interest in including information related to other types of licences (such as marine licences) or evidence of identity documents (such as proof of age cards) to support their issuance processes and investigative/de-duplication activities. Whether these additional data fields are returned in the response to external queries is a matter for data sharing agreements, informed by privacy impact assessments. There is the technical ability to configure the NDLFRS and Hub depending on what is agreed and permitted by legislation.

Each RTA is able to replicate core data and optional data as agreed in the information exchange agreements (conditions and other licence specific fields are considered optional).The table below provides a list of the mandatory and optional data items that each RTA may replicate into their own dedicated partition within the NDLFRS.

Mandatory Data Items	Optional Data Items
- Facial image - Last name - Date of birth - Gender - Document and card numbers - Document type - Image number	- Given name(s) - Deceased status - Current address only - Document status - Issue and expiry date - Licence class (i.e. learner, probationary) - Endorsements (i.e. instructor) and conditions (i.e. automatic vehicle only) - Card status (i.e. active, suspended)

3.3.1.2 Personal information flows for NDLFRS based Face Matching services

Figure 2 – Data flow diagram for Face Verification Service

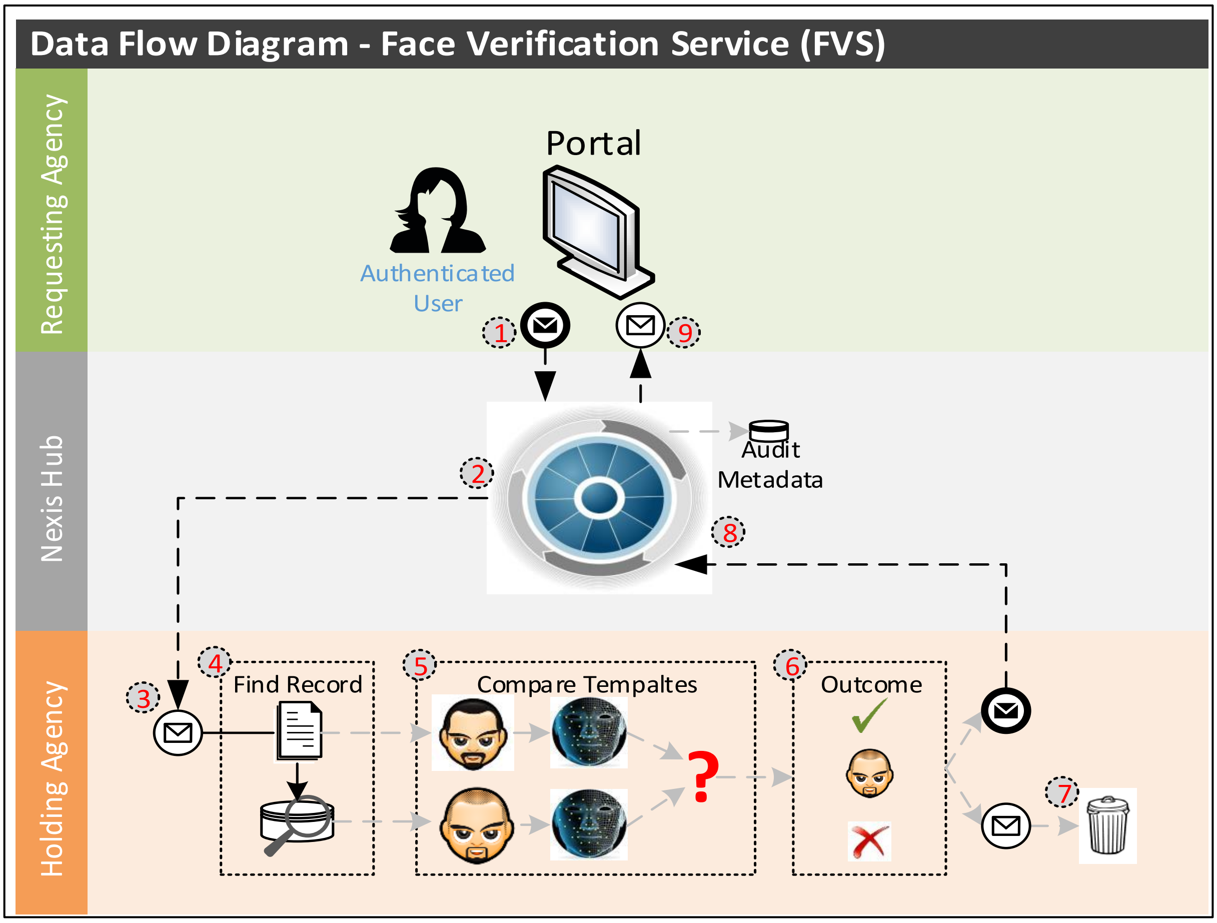


Figure 3 – Data flow diagram for Face Identification Service

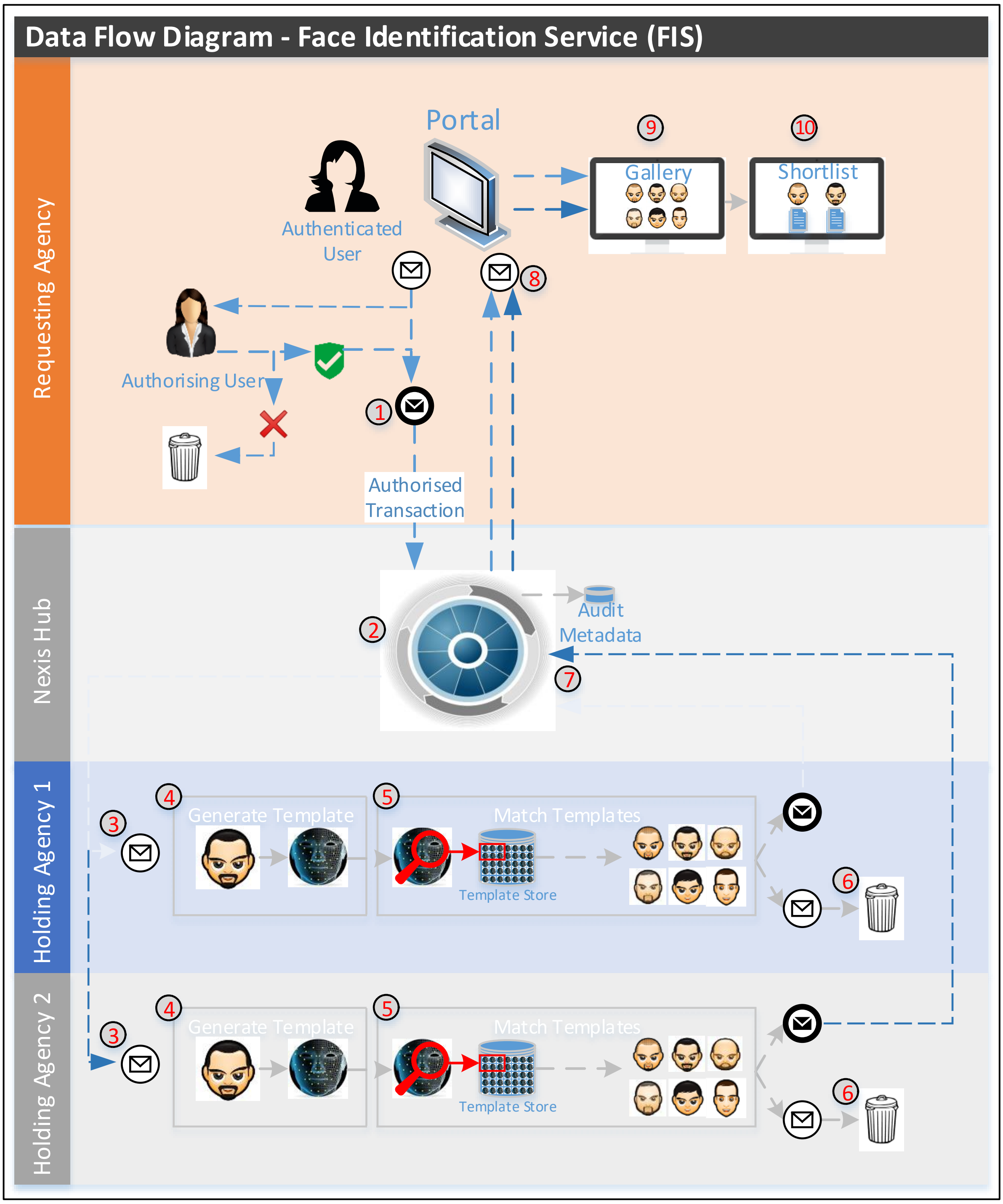
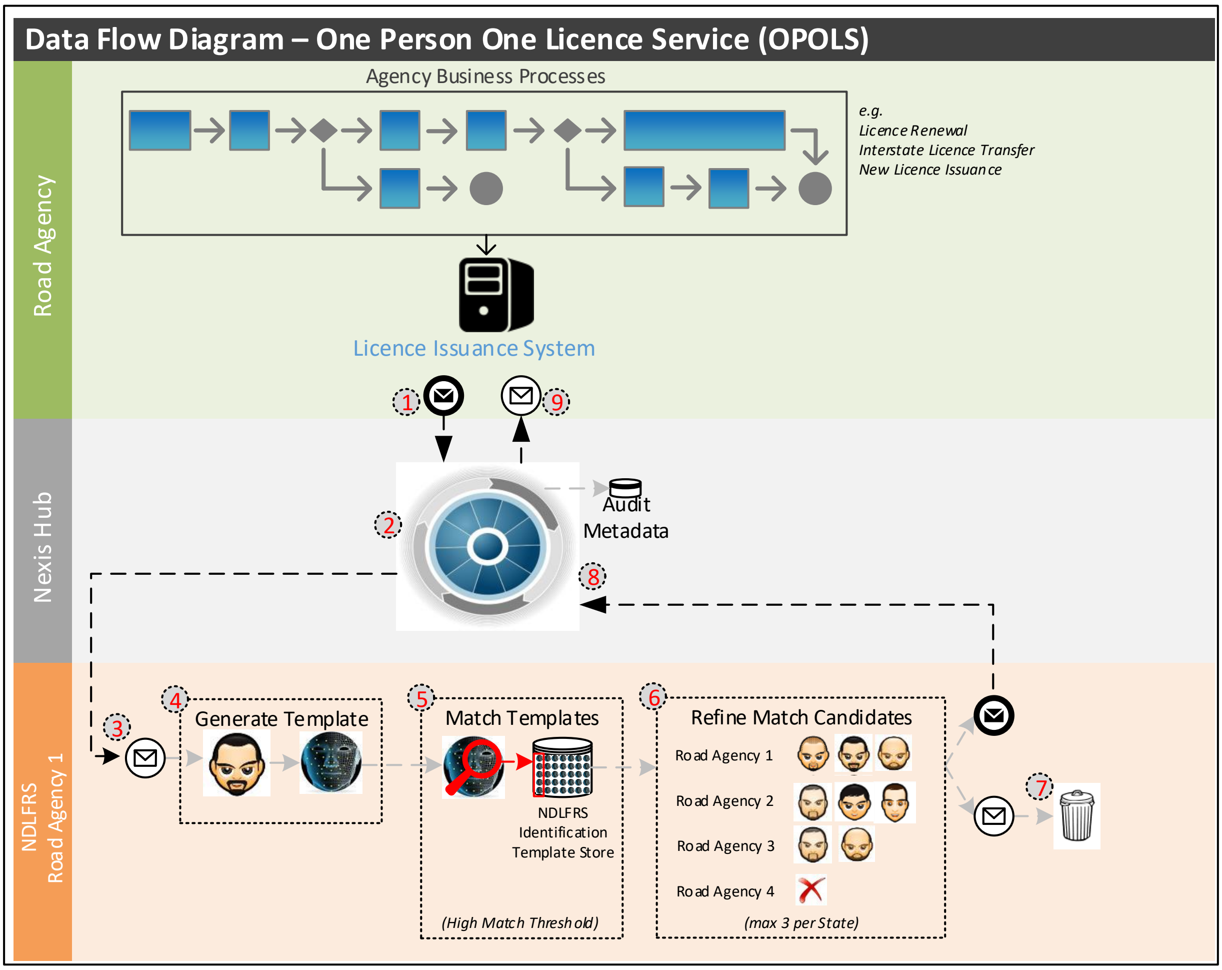


Figure 4 – Data flow diagram for One Person One Licence Service



Detailed tables that describe the information flow at each step of the FVS, FIS and OPOLS transactions can be found at Appendix D.

3.3.1.3 Information generated in relation to NDLFRS transactions

The Hub retains in its audit logs transaction data such as: transaction type; Requesting Agency; Data, Holding Agency which received the request; the unique values of the results returned; and date/time stamps - but the Hub audit logs do not contain any personal information at all.

The Hub logs data on all transactions in a manner that is privacy respecting while also ensuring requesting agencies can monitor use of system and investigate anomalies. The Hub does not store any biometric, biographic information or driver licence information about individuals (although the information collected in audit logs could act as a ‘pointer’ to such information held by participating agencies). The Hub also retains the MD5 message-digest algorithm or cryptographic hash for each image with the intention of further facilitating audit or investigation activities by participating agencies.

The Hub audit data alone is insufficient to construct any meaningful history of the pattern of access to a particular image. An administrator would need to have access to Hub audit data, requesting and holding agency audit data to accumulate and piece together the information required to recreate transactional history against a specific probe image. No single administrator has all this access.

To enable comprehensive auditing, as well as the ability to reconstruct a match request if required, the NDLFRS will need to contain more detailed audit information than the Hub. The NDLFRS collects two types of audit information, namely:

- Database-level audit information relating to the specific data items that are replicated from each RTA to their own dedicated partition. Logs are kept to ensure that the NDLFRS holds the most up-to-date records, and to detect any failures in the data replication processes. These audit logs will only be made available to the relevant RTA (i.e. RTA-B cannot access the database-level audit information from RTA-C).
- The audit information generated by the facial recognition software when it processes match requests.

It is proposed that the audit data generated by the facial recognition software should include similar transactional metadata to that collected by the Hub (i.e. date, time, reference numbers etc) as well as the biographic data (i.e. name and date of birth) of the particular individual(s) whose information was disclosed in response to a match request. For privacy and security reasons, it is proposed that the biographic data would be stored separately to the transactional metadata.

Subsets of this audit data would then be made available to participating agencies in accordance with the audit requirements outlined data sharing arrangements and supporting policies. For example, in the case of an audit of Agency A's use of a Face Matching Service against RTA-B, both the Hub and NDLFRS facial recognition software audit data relating to Agency A's use would be provided. This would enable a full end-to-end audit of the data that were disclosed to Agency A, at particular times and for the specific purposes in accordance with their data sharing agreement.

The table below provides an outline of audit data collected within the Hub, and the proposed audit data collected by the facial recognition software within the NDLFRS. A detailed list of the audit fields can be found in Appendix C. This information will only be retained for the minimum length of time as required by law.

Hub Audit Data	Proposed NDLFRS Audit Data
• Transaction date/time • Function ID (i.e. FVS/FIS) • Transaction group ID • Transaction ID • Data source ID (i.e. passports) • Holding agency ID (i.e. DFAT) • Transaction status (i.e. submitted, received, delivered, returned etc) • Requesting agency ID (i.e. AFP) • System user ID (i.e. portal, RTA licence issuance system) • User ID (i.e. AFP123)	• Transaction date/time • Function ID (i.e. FVS/FIS) • Transaction group ID • Transaction ID • Data source ID (i.e. RTA-B driver licences) • Holding agency ID (i.e. RTA-B) • Transaction status (i.e. submitted, received, delivered, returned etc) • Requesting agency ID (i.e. AFP) • System user ID (i.e. portal, RTA licence issuance system) • User ID (i.e. AFP123)

• MD5# value of the probe image • MD5# value(s) of returned images • Message state (i.e. success, fail, error etc) • Message state message (i.e. request timeout) • Permitted purpose category and specific purpose (i.e. law enforcement – homicide) • Enabling legislative provision • Authorising officer ID (i.e. AFP456) • Internal reference number	• MD5# value of the probe image • MD5# value(s) of returned images • Message state (i.e. success, fail, error etc) • Message state message (i.e. request timeout) • Permitted purpose category and specific purpose (i.e. law enforcement – homicide) • Enabling legislative provision • Authorising officer ID (i.e. AFP456) • Authorisation override indicator • Supervising officer ID (i.e. AFP678) • Subject of request (i.e. POI, witness, victim) • Minor searched indicator • Max results indicator • Match threshold • Internal Reference Number In a separate audit database for match responses: • Name • Date of birth • Transaction ID

3.3.1.4 Information held in the NDLFRS template database

As well as the template itself, the Template Database would store a Template ID and a Face Recognition (FR) Entity ID value. The Template ID is a unique pointer to the biometric template of the image, and the FR Entity ID associates an individual licence holder with the Template.

3.4 Security and privacy protection measures

The privacy and security protections for the NFBMC and the NDLFRS include a combination of design and technical measures together with legislative and policy controls. An overview of the protections is as follows.

3.4.1 Design and technical measures

Key privacy design and technical features for the NFBMC include:

- The Hub and spoke architecture
- No personal information retained in the Hub
- Clearly delineated services (FVS, FIS and OPOLS)
- No face recognition from live video.

The NDLFRS would effectively be a large new centrally held database. Offsetting this are system design and technical features as follows:

- Partitioned databases – driver licence images, biographic information and related driver licence information are accessible only to the owning RTA and are stored in partitioned databases
- Full control of data – each RTA retains full control over the data replication processes and their partitioned database, such as to set their own rules for access
- Data not accessible by AGD – while AGD hosts the system on behalf of the all RTAs, the images and biographic and related driver licence information within is not accessible to AGD, except via the Face Matching Services where this is specifically agreed by states and territories.

3.4.2 Security measures

The NDLFRS adopts best practice security and access arrangements in accordance with the Australian Government's Protective Security Policy Framework and the Information Security Manual. This includes:

- independent penetration and vulnerability tests as well as ongoing testing
- a full independent security review by the Australian Signals Directorate
- formal Information Registered Assessor Program (IRAP) certification and annual reassessment
- ongoing 24/7 monitoring and state-of-the-art encryption, anti-virus and intrusion detection in accordance with the requirements of an information technology system classified as 'Protected'
- physical and personnel security arrangements in accordance with Zone 4 (Secret) requirements.

There are also a range of specialised security and access controls, with user-level privileges that the system enforces down to a very granular level, with system access re-justified:

  - For the FIS (one to many matches) every 90 days
  - For the FVS (one to one matches) every 180 days

- All information and communication between parties passing through the NDLFRS are in encrypted form
- Comprehensive audit records, including metadata about the transactions (including, User ID, date and time of transaction, MD5 hash of the image being searched, service accessed) would be maintained for audit and oversight purposes.

3.4.3 Privacy measures

There is a range of interacting policy and legislative measures that together would help protect the privacy of information held in the NDLFRS. These include:

- Annual audit as part of AGD's management of the NDLFRS
- Published annual reports on usage of the Face Matching Services by government agencies and private sector organisations in each financial year
- Proposed review of the of the operation of the Identity Matching Services every three years, including the privacy impacts and effectiveness of privacy safeguards
- Statutory review of the operation of the legislation governing the Identity Matching Services (to commence within five years of commencement of the legislation).

Additionally, the use of NDLFRS data by a requesting agency would be subject to the following privacy safeguards:

- The scope of the information sharing is defined at a high-level within the intergovernmental agreement that sets out the specific set of identity matching services through which information may be shared
- Information sharing would be subject to the terms and conditions of a common Face Matching Services Participation Agreement between participating agencies, with legally binding privacy safeguards as well as audit and oversight obligations
- Requesting agencies must demonstrate that their collection, use and disclosure of personal information has a lawful basis.

NDLFRS use would also be subject to the following existing NFBMC safeguards:

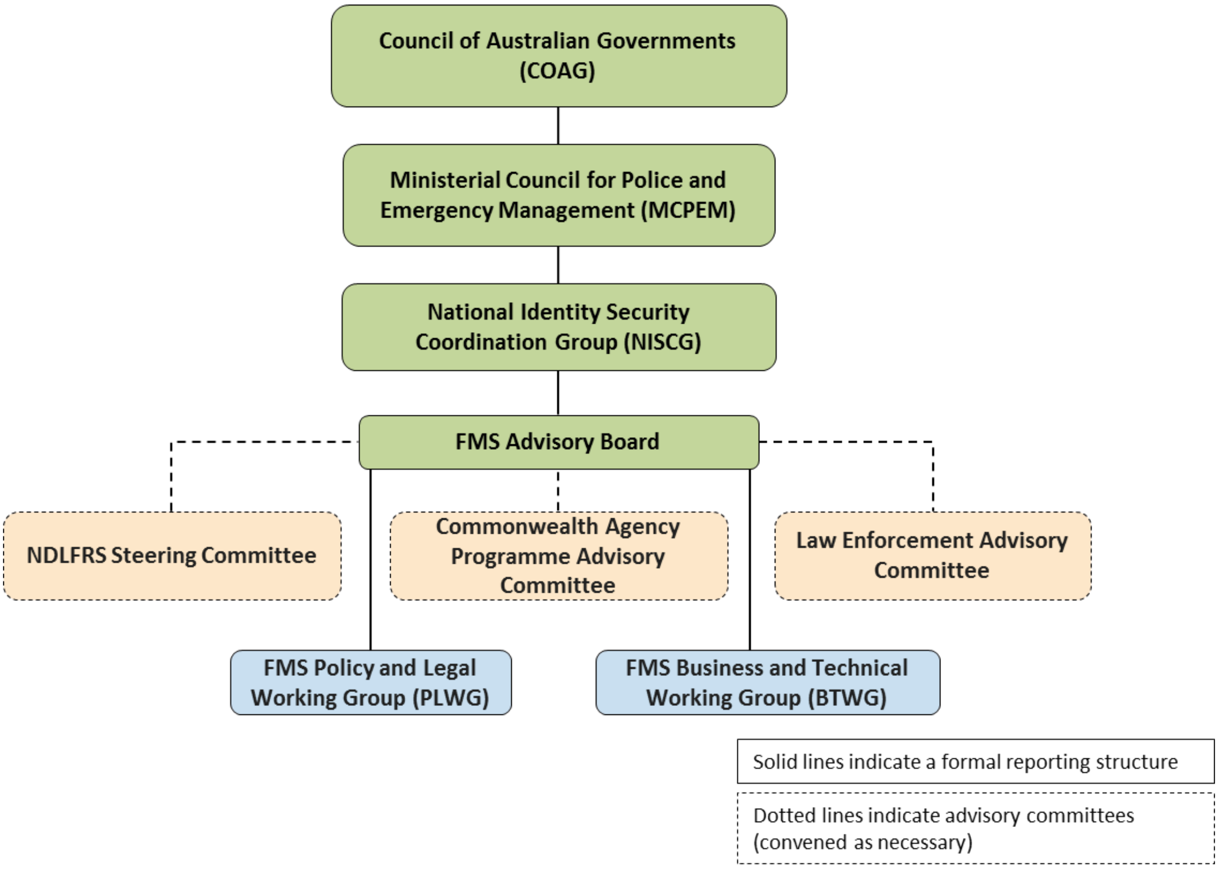
- The face match results delivered by the NFBMC are not intended to be evidentiary – they cannot be relied on as the exclusive means of identification, thereby limiting the risk that decisions would be taken without testing the accuracy of the match
- Requesting agencies' access to the services is subject to a PIA to be published
- Users in requesting agencies are required to undergo training on security and privacy obligations.

3.5 Proposed governance arrangements

An *Intergovernmental Agreement on Identity Matching Services* (IGA) will govern the operation of the NDLFRS. This IGA was agreed by COAG in early October 2017, and outlines the policy, legislative and financial arrangements supporting state and territory participation in the Face Matching Services, including but not limited to the NDLFRS.

Governance and ministerial oversight would be provided by the Ministerial Council for Police and Emergency Management (MCPEM), which is a body comprising Commonwealth, state and territory Ministers who have responsibility for justice and/or police portfolios. Supporting the Ministerial Council is the National Identity Security Coordination Group (NISCG), which comprises senior officials at the APS equivalent of Deputy Secretary/CEO level, or their representatives. The NISCG is supported by the Face Matching Service Advisory Board, which comprises of officers at the APS equivalent of SES Band 1. Figure 5 below illustrates the governance structure.

Figure 5 – Overview of Governance Structure


Council of Australian Governments (COAG)
Ministerial Council for Police and Emergency Management (MCPEM)
National Identity Security Coordination Group (NISCG)
FMS Advisory Board
NDLFRS Steering Committee
Commonwealth Agency Programme Advisory Committee
Law Enforcement Advisory Committee
FMS Policy and Legal Working Group (PLWG)
FMS Business and Technical Working Group (BTWG)
Solid lines indicate a formal reporting structure
Dotted lines indicate advisory committees (convened as necessary)

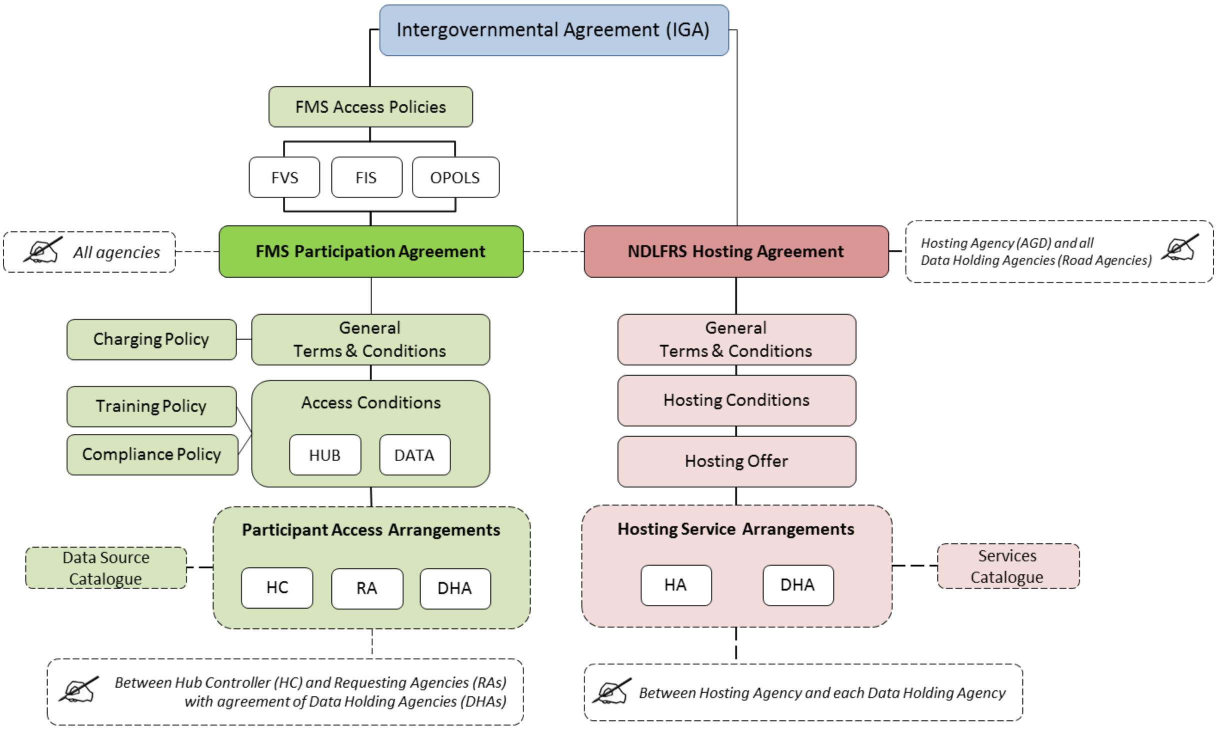
Information sharing via the Face Matching Services, including data held with the NDLFRS and other data sources, would also be subject to enforceable agreements.

Rather than numerous different bi-lateral data sharing agreements, AGD is developing a multi-lateral *Face Matching Services Participation Agreement* that outlines the roles, rights and obligations of agencies participating in the Face Matching Services, whether they are Data Requesting Agencies, Data Holding Agencies, or the agency (currently AGD) that manages the Interoperability Hub.

The Participation Agreement would incorporate the Access Policies developed for each of the Face Matching Services to provide a framework of common terms and conditions, within which agencies would negotiate the specific details of their Participant Access Arrangements.

The Commonwealth would also enter into an *NDLFRS Hosting Agreement* with RTAs to outline the specific terms and conditions under which data is held in the system and under which the system can be used by RTAs to search and analyse their own data. Figure 6 below provides an overview of the agreements structure and supporting policies.

Figure 6 – Overview of Agreement Structure and Supporting Policies


Intergovernmental Agreement (IGA)
FMS Access Policies
FVS
FIS
OPOLS
All agencies
FMS Participation Agreement
NDLFRS Hosting Agreement
Hosting Agency (AGD) and all Data Holding Agencies (Road Agencies)
Charging Policy
General Terms & Conditions
Training Policy
Compliance Policy
Access Conditions
HUB
DATA
General Terms & Conditions
Hosting Conditions
Hosting Offer
Data Source Catalogue
Participant Access Arrangements
HC
RA
DHA
Hosting Service Arrangements
HA
DHA
Services Catalogue
Between Hub Controller (HC) and Requesting Agencies (RAs) with agreement of Data Holding Agencies (DHAs)
Between Hosting Agency and each Data Holding Agency

3.6 Proposed legislative framework

The Commonwealth will introduce legislation to support the NFBMC program, including the NDLFRS. AGD anticipates the legislation would cover matters such as the types of services, permitted users and purposes, as well as privacy and other safeguards. The legislation is intended to authorise the agency hosting the NDLFRS and the Hub to collect, use and disclose personal information for the purpose of providing the Face Matching Services. It is not intended to increase the powers of agencies using the Face Matching Services to collect personal information.

The proposed legislation is subject to a separate PIA and is not within scope of this PIA being conducted on the NDLFRS.

3.7 AGD's role in relation to NDLFRS information

AGD would be designated as the NDLFRS hosting agency. Its ongoing role is to keep the system running, coordinate the governance arrangements, undertake annual audits, provide help desk arrangements etc.

AGD would be a facial recognition services provider to RTAs, to analyse their own data holdings, and a provider of the Face Matching Services to all participating agencies. It has responsibility for managing the underlying systems and services, as well as the overarching policy, governance, access and privacy arrangements.

AGD does not have the technical ability to access the RTAs' data within the NDLFRS directly and this would be enforceable via contractual arrangements with the RTAs.

In a similar manner to both the DVS Hub and Biometric Hub, AGD has a managed service arrangement with a private sector provider. The provider does have the technical ability to access RTA data, however this is not permitted under the contractual arrangements with the provider. Legislation proposed to support the NFBMC would create a criminal offence for unauthorised use or disclosure of information by staff or contractors of the agency hosting the Hub or NDLFRS.

Jurisdictional representatives approve who can access their data under what circumstances and this is activated technically within the Hub and/or NDLFRS.

4. Stakeholder consultations

AGD asked IIS to consult:

- Commonwealth, state and territory privacy commissioners, or their equivalents
- Representatives from state and territory RTAs.

IIS was not asked to consult more widely. The consultations involved a round table meeting with each of the groups. AGD gave a presentation on the NFBMC, including the proposed NDLFRS functionality, privacy protections, legal framework and governance arrangements and this was followed by round table discussions. The stakeholders were also invited to make further written submissions as input to the PIA following the initial consultation. The draft PIA report was also provided to stakeholders for comment.

Details of the bodies consulted and additional submissions made are at Appendix C, Section 9.1.

A summary of matters raised in the consultations and submissions by privacy regulators is at Appendix C, Section 9.2 and by RTAs is at Appendix C, Section 9.3.

IIS's PIA takes account of the matters raised by stakeholders to the extent that the issues were in scope for this PIA. Some issues, including the appropriate legislative framework for the NDLFRS and RTA's use of the NDLFRS were outside the scope of this PIA.

IIS reviewed all feedback on the draft PIA and, where needed, sought clarification and additional input from AGD. Based on the feedback IIS made a number changes including adding information or clarifying points.

IIS notes that the views expressed in this report are its own. Where the PIA refers to points raised in the stakeholder meetings and submissions it is not intended to represent the views of the privacy commissioners or the RTA representatives.

5. NDLFRS Benefits

IIS' preliminary PIA on the NFBMC Interoperability Hub noted the range of expected benefits from the development of the Hub and its Face Matching Services that had been identified by AGD. The Hub is designed to foster more efficient collaboration between agencies using biometric systems across government by facilitating the secure, automated and accountable exchange of identity information. AGD expected this to help prevent or manage fraud and identity crime (which is estimated to cost

Australia $2.6B per year), as well as to promote law enforcement, national security, road safety, community safety and service delivery outcomes.

The addition of the NDLFRS is expected to enable the achievement of the full range of anticipated benefits as well as delivering specific capabilities to RTAs. The NDLFRS could assist RTAs to undertake identity verification more easily. RTAs should also be able to implement their OPOLS policy better, and detect attempts at fraud or sanction avoidance, by performing matching across other jurisdictions' driver licence records. Further, RTAs would be able to access state-of-the-art facial matching technology via facial recognition tools with a widened pool of facial matching expertise to analyse their own data holdings to assist in data integrity analysis and remediation.

The benefits and the allocation of an appropriate component to the NDLFRS initiative, as well as the system costs are estimates only. AGD is continuing to develop a benefits and costs methodology.

6. NDLFRS privacy risk analysis and recommendations

6.1 IIS' approach to risk assessment for this PIA

Consistent with the scope for the PIA, IIS has focussed its risk assessment on the design, operation and governance of the NDLFRS.

In assessing privacy risks for the NDLFRS, IIS has used the requirements of the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth) (Privacy Act) as its initial framework for analysis. The table at Appendix E canvasses possible privacy risks for the NDLFRS design, operation and governance against the APPs.

IIS has also considered broader privacy risks, for example, the allocation of privacy risks and possible broader community concerns about the impact of the information flows.

The NDLFRS would be the most significant input of images into the NFBMC as well as adding to the number of users or Requesting Agencies. IIS' risk assessment takes account of relevant aspects of its preliminary PIA of the NFBMC.[3] Of particular relevance are its recommendations on the NFBMC governance arrangements and AGD's responses to those recommendations.[4]

The main areas of risk identified are of risk discussed below.

[3] See https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Privacy-Impact-Assessment-National-Facial-Biometric-Matching-Capability.PDF

[4] See https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/AGD-response-privacy-impact-assessment.pdf

6.2 NDLFRS design issues

IIS' privacy assessment was undertaken on the architecture that AGD has adopted and is now implementing for the NDLFRS. IIS understands that in progressing the development of the NDLFRS AGD used the following design principles:

- The system should be designed to maximise performance, with a minimum number of bandwidth chokepoints
- A consolidated system architecture is essential, but de-centralised control of data is preferred
- Avoid the creation of a 'honeypot' of assumed identities – dynamic management and alerting is essential
- The design must adopt best practice security policies, and role-based access control is vital
- The technical solution should be highly available and robust, scalable, standards based and fit for purpose.

The various design options considered had varying degrees of centralised co-location versus decentralised location within jurisdictions of the key elements of the NDLFRS, which are:

- The facial matching engine
- The repository (or repositories) of biometric templates of the driver licence images for each of the states and territories
- The database (or databases) of the driver licence facial images and biographic and related drivers licence information for each of the states and territories.

As outlined in detail in Section 3.2, the model chosen was a consolidated facial matching engine and replicated repository of templates, with segmented database of facial images and biographic and related drivers licence information (see Figure 1 above). This model was considered to best meet the identified design principles. AGD also advised that it was the most cost effective approach.

The model does mean that AGD would be holding a replicated set of driver licence images and biographic and related drivers licence information for all Australian jurisdictions.

IIS considers there are potentially significant privacy risks in this model; the centrally held database could be a honeypot for hackers or other nefarious purposes, there are security risks in the data transfer process, central holding might more easily suggest additional uses of the data and data accuracy issues might be less easily managed. However, it also recognises that there are likely to be both privacy pros and cons for other more centralised or decentralised models and related data storage and transfer arrangements and management approaches.

IIS also notes the very strong intention for states and territories to remain in control of their data and for a robust set of measures to reinforce this and to protect the information in AGD's hands. IIS considers that the risks are manageable subject to the delivery of the range of technical, legal and policy privacy safeguards that are outlined in Section 3 above and subject to the recommendations it makes with respect to the NDLFRS operation and governance.

IIS has not identified other specific privacy risks for the NDLFRS and does not make recommendations in relation to the NDLFRS design.

6.3 NDLFRS Operational issues

This section considers the technical implementation of face matching requests, AGD's role and responsibilities and RTA responsibilities and obligations (which include data accuracy, privacy notices to individuals and handling inquiries and complaints) as far as they affect agreements and processes.

6.3.1 Application of Privacy Act and APPs

A key design feature for the NDLFRS is that AGD would hold the replicated driver licence data on behalf of the states and territories. AGD's role in relation to driver licence information would be governed by the IGA at a higher level, with more detailed enforceable protections in the NDLFRS Hosting Agreement. As noted earlier, it would have a management role only and would not have direct access to the driver licence information.

The clear intention is that the RTAs would remain in control of the information in their partitions, particularly any decisions on whether and how this information is shared with other agencies via the Face Matching Services. IIS sees this as an important privacy protection against what could otherwise be a new database available for possible reuse within the Commonwealth. IIS considers that the governance arrangements proposed support this approach and it does not have additional recommendations. However, any change should be subject to a transparent PIA process.

IIS understands that AGD considers the Privacy Act and the *Freedom of Information Act 1982* (Cth) (FOI Act) would apply to the NDLFRS information it holds and for the purposes of the Privacy Act AGD would be collecting, using and disclosing the personal and sensitive information that RTAs replicate into their partition. The proposed Commonwealth legislation is also intended to ensure, amongst other things, that AGD's role in handling driver licence information in the context of the NDLFRS is consistent with the Privacy Act.

While these factors should reinforce AGD's commitment to maximising privacy protections for the information held in the context of the NDLFRS, IIS notes that AGD considers that the approach means that state and territory privacy or freedom of information regimes are not applicable to the information it holds. A practical difficulty then arises; AGD does not have direct access to any of the NDLFRS data that it holds and therefore would be constrained in its ability to respond to privacy or security issues. AGD advises that it would work with the states and territories to respond to any freedom of information (FOI) requests, individual requests for access or correction under the Privacy Act, or privacy complaints. It is currently developing policies and procedures to give effect to this intention (see Section 6.3.5 below).

IIS considers that if there is any doubt about which privacy or FOI law applies or if practical or procedural issues arise because AGD does not have direct access to the data, there is real potential for issues to fall between the cracks or to cause difficulties for individuals in exercising their privacy rights. The application of privacy and FOI law to NDLFRS data in AGD hands should preferably be clarified in law or, noting that there could be constitutional limits in the ability for Commonwealth legislation to impose responsibilities on states and territories, in the IGA and legally binding participation and/or hosting agreements.

In particular, IIS considers that AGD should ensure that there are no inadvertent impacts of the legal provisions or administrative approach, for example, on individuals' right to pursue a privacy complaint or seek to exercise FOI rights under either a state or territory privacy law or Commonwealth law.

Recommendation 1 – Ensuring RTAs control NDLFRS information and individual rights are maintained

IIS recommends that AGD ensure that:

- Any changes to the NDLFRS administrative or legal arrangement that could affect the extent to which the states and territories remain in control of information in their partitions of the NDLFRS should be subject to a transparent PIA process
- The application of privacy and FOI law to NDLFRS data in AGD hands, including the respective roles and responsibilities for the Commonwealth and states and territories, should be clarified in law or in the IGA and legally binding participation and/or hosting agreements
- Individuals are not disadvantaged by any inadvertent impacts of the legal provisions or administrative approach, for example, on individuals' right to pursue a privacy complaint under a state or territory privacy law.

6.3.2 APPs – Collection, use and disclosure

In keeping with its PbD approach, AGD has aimed to minimise the amount of information held and used in the context of the NDLFRS, taking account of other factors, such as cost and efficiency. This approach would be reflected in the proposed Commonwealth legislation to support the NFBMC, which would define 'identification information'.

While it is outside of the scope of this PIA to consider the proposed legislation, IIS supports the intention to define and limit identification information, particularly where such information is categorised as sensitive in the Privacy Act.

IIS has considered the collection and handling of information as it relates to the NDLFRS operations. The issues it has identified are discussed below.

6.3.2.1 APPs – Transparency and privacy notices

PbD principles as well as the APPs emphasise transparency. The APPs call for both general privacy policies and also for organisations to take reasonable steps to let people know information about them has been collected and why. This principle applies whether collecting information directly from the individual or from another body. The level of effort needed would depend on the nature of the information and the circumstances in which it is collected and would be used.

The use of face matching in government administration and law enforcement is a relatively new initiative and one that is unlikely to be well understood in the community. Individuals are also unlikely to know that their driver licence information would be copied to AGD for use in face matching activities. In these circumstances, there is a need for specific transparency measures.

Although AGD would not have direct access to the NDLFRS data, as noted it considers it would be collecting and holding personal information on behalf of the states and territories, and personal information would be used and disclosed via the Face Matching Services. AGD would therefore have obligations under APPs 1.3 and 5 to provide information about its NDLFRS activities.

IIS understands that AGD would be relying on states and territories to give privacy notices when they are collecting information that would be transferred to the NDLFRS. The IGA provides that:

> When individuals apply for new or renewed driver licences (or any other documents containing facial images to be used in the National Driver Licence Facial Recognition Solution) Road Agencies (or other relevant licencing agency) will take all reasonable steps to notify these applicants that the personal and sensitive information being collected by the Road Agency may be disclosed for the purposes of biometric matching through the National Driver Licence Facial Recognition Solution for law enforcement, national security and other purposes.[5]

IIS supports this requirement. However, there was some uncertainty in the stakeholder meetings about the level of detail that would or could be provided. IIS' view is that notices should be explicit, consistent across jurisdictions and non-discretionary.

An additional factor, raised by Office of the Australian Information Commissioner (OAIC) and also the Queensland road agency, the Department of Transport and Main Roads, is that while the IGA's notice provision will ensure notices are provided to new driver licence applicants, it will not deal with the historical information. As noted in submissions, there can be lengthy periods where individuals will not interact with RTAs; for example, it might be 10 years between driver licence renewals.

AGD's obligations under APPs 1.3 and 5 would apply to drivers licence information already held as well as for new licences going forward. IIS agrees that for this reason either AGD or RTAs would need to proactively notify individuals about the operation of the NDLFRS.

In addition, while AGD's website does include reasonably detailed information about its Face Matching Services these are not mentioned in its privacy policy. IIS considers the privacy policy should mention the services. It also considers that AGD should take additional steps to ensure it is transparent about its role and to support steps to promote community understanding and awareness of Face Matching Services and how individuals can get help if needed.

Recommendation 2 – Transparency and information for individuals

IIS recommends that AGD work with the NISCG and participating organisations to ensure that the IGA or the NDLFRS Hosting Agreement include non-discretionary requirements for RTAs to provide explicit up-front notice to future driver licence applicants about the Commonwealth's collection of driver licence images for biometric face matching for law enforcement, national security and other

[5] IGA, October 2017, Clause 6.19

purposes. In addition, IIS recommends that either AGD or RTAs take proactive steps to notify individuals whose information is already held by RTAs about the inclusion of their information in the NDLFRS. This could involve mail-outs to individuals and/or a public education campaign.

IIS also recommends that AGD develop and disseminate information, for example in its privacy policy, and via its website, or brochures distributed by RTAs, that provides specific details on the information that would be collected for the NDLFRS and how it stored and used and the associated privacy safeguards. Information about how individuals can seek help to resolve any identity problems arising as a result of use of the NDLFRS should be included.

6.3.2.2 APPs – Consent

The APPs permit collection, use and disclosure of biometric information where authorised by law and in other circumstances, including where individuals have given their consent.

Consent approaches were discussed with the privacy regulators. The starting point was that where consent is the mechanism for authorising collection, use and disclosure of information a best practice approach is needed. In the NDLFRS context there was discussion about whether best practice (and possibly the law) required having viable alternatives channels for identity verification.

Discussions with AGD, privacy regulators and RTAs about driver licence issuing indicated there could be options to present at an office with identity documents. However, the NSW RTA emphasised its view was there would be no legal requirement to offer this and it was not clear that such alternatives would be consistently available or practical for all identity verification requirements.

Some regulators considered that it would be better to recognise the practical difficulties in offering 'real' consent and focus instead on strengthening other privacy protections. For example, in a follow-up submission the Victorian Commissioner for Privacy and Data Protection noted that:

> Relying on consent as legal authority to collect, use and disclose personal information is not the only way to demonstrate to citizens that government values their privacy. Ensuring that the most rigorous privacy and security control are built into the NFBMC and the NDLFRS platforms to protect the integrity and confidentiality of facial images can provide more meaningful assurance to individuals that their information will be used appropriately than the fact that they have given consent. This must be coupled with a transparent approach to informing citizens of the purposes of face verification.

In the context of the NDLFRS, the 'authorised by law' path will often apply and consent, as such, will not come into play. IIS understands, for example, that the proposed Commonwealth legislation will authorise AGD's collection of information for the NDLFRS. IIS also recognises that for driver licence issuing and similar services, identity verification is mandatory and that in these and similar cases identity resolution is utterly justified.

However, there would be circumstances where there is no justification for mandatory identity resolution and agencies or organisations would need consent to verify an image against NDLFRS holdings (via the Face Verification Service, facilitated by the Hub). IIS notes that the Commonwealth

Digital Service Standard builds in such a requirement from a customer service perspective. [6] Agencies are required to 'ensure that people who use the digital service can also use the other available channels if needed, without repetition or confusion'.

IIS strongly support the approach that where consent is intended to be the authorising mechanism, alternative mechanisms would, consistent with the Digital Service Standard, support real choice.

Recommendation 3 – Requirements for consent based access to NDLFRS

IIS recommends that AGD work with the NISCG and Participating Agencies to ensure that where organisations are permitted to use the FVS to access facial images from the NDLFRS on the basis that individuals have given their consent:

- The consent must be express, freely given and fully informed
- Consistent with the Commonwealth Digital Service Standard, there must be a viable alternative method available for individuals to authenticate or verify their identity
- This requirement is included in the proposed legislation for the NFBMC.

6.3.3 APPs – Accuracy

6.3.3.1 Accuracy and face match failures

Stakeholder discussions identified data accuracy, and the accuracy of face matching processes, as a significant privacy risk for the NDLFRS. Both could lead to false negative or false positive face match results, with the potential impact for individuals.

Facial recognition is not an exact science; there is seldom a 100% or 0% match. The results depend on the quality of the 'probe' image submitted as part of a matching request, the quality of the 'reference' image contained in the NDLFRS, and the defined matching threshold; that is the cross over point between a match and no match.

AGD has built in a range of measures aimed at minimising the risk and impact of false negatives or false positives; these include access policies, staff training, system design and testing, including biometric matching threshold testing. It will be setting the thresholds, depending on matters including the type of request; the FVS and FIS will have different threshold values. It is also working with the states and territories to test its face recognition engine against their data sets.

AGD advised that data quality is an issue for the NDLFRS implementation processes. States and territories have identified duplicate records and other integrity issues and there are some record-keeping variations between the jurisdictions. AGD expects that increasing use of OPOLS and FRAUS

[6] The Digital Service Standard (the Standard) applies to federal Government agencies when developing new information and transactional services and for all high volume transactional services (for example, lodging a tax return online). See https://www.dta.gov.au/standard/

would help improve data quality over time. However, this is expected to be long-term process as licences are renewed or transferred over a number of years. Cost and other practicalities mean there is no intention for a wholesale across the board de-duplication process to clean up data.

It is also important to note that while AGD hosts the road agency data, and as OAIC notes will help to ensure the accuracy of the information held within its system by setting and enforcing threshold accuracy levels, it does not have the ability to update or change any information. RTAs remain responsible for the accuracy of their data, and the process of changing records, for example following the discovery of inaccuracy, must occur in the road agency master system and then an update replicated through to their partition within the NDLFRS.

A key part of the stakeholder discussions was likely processes to resolve match failure issues for individuals, particularly where there are multiple jurisdictions involved. Factors that could affect outcomes for individuals included inconsistent business processes between the jurisdictions, co-ordination between jurisdictions and resources and contacts available. IIS considers that a privacy success criterion for the NDLFRS would be to ensure that processes do not transfer risks from the RTAs, or other Requesting Agencies, to the individuals. This could occur, for example, if processing takes longer or if individuals have to go to multiple agencies to resolve issues.

It is also not yet clear whether there would be legal impediments in any of the jurisdictions to data sharing for the purposes of handling complaints (as opposed to RTA or law enforcement related inquiries).

AGD advised that each requesting user/agency would define their own exception handling processes; these would depend on the functions and services they have available. For example:

- OPOLS has been designed as a background process initiated from within an RTA's own licence issuance system. Trigger events may include licence renewal, interstate transfers, or requests for new licence. Results – if any – would be routed to a back office specialist unit, with staff trained in face recognition for assessment. OPOLS transactions can be a real time check or overnight batch job, as best suits the Road Agency business practices. In most cases, it is more likely to be overnight; only Northern Territory and the ACT now issue on the spot licences, other jurisdictions give a temporary two to three week paper licence and post the actual licence out once all checks are done.
- Requesting Agencies could conduct different FVS functions (where able) to assist with the triage of exception cases. For example, if an FVS Match request was unsuccessful, an FVS Retrieve transaction (ideally with consent) might be allowed/required to obtain the relevant image to try and validate the Data Holding Agency record. Otherwise the Requesting Agency would need to contact the Data Holding Agency for case resolution.

Each RTA would also have its own help desk support arrangements. Discussions with the RTAs indicated these may need to be enhanced, in some cases possibly significantly.

The privacy regulator discussions, and later submissions, also raised the issue of the handling of privacy complaints given the centralisation of driver licence data and the consequent intersection of roles and responsibilities for information and processes. For example, the Northern Territory Information Commissioner assumed that:

- A complaint about data quality would be dealt with by the Northern Territory (and similar jurisdictions)
- A hardware or software failure (of the Hub or NDLFRS) is a matter for the Commonwealth, with oversight by the OAIC.

The discussions with AGD and other stakeholders indicated awareness of the issues and possible difficulties for individuals in negotiating the system. While there was confidence that processes for resolving face match difficulties or resolving complaints would be in place, these matters are still to be settled. Ensuring sufficient resources are available would be a significant factor. Also important is the risk that individuals would need to approach a number of agencies in different jurisdictions to resolve issues with their identity following a face match fail.

Recommendation 4 – Process to handle false negative matches

IIS recommends that AGD work with Road Transport Agencies to develop a strong privacy approach to the handling of ‘no match’ or error responses following a face match request using the NDLFRS by doing such things as:

- Undertaking risk assessments to identify issues that might arise for individuals
- Encouraging consistent business processes across all jurisdictions
- Identifying agreed benchmarks for resolving issues and ensuring resources are available to meet the benchmarks
- Requiring each jurisdiction to have resources available to resolve issues for their own customers and to respond to requests from other jurisdictions within a reasonable time frame. Each jurisdiction should also provide up-to-date details for a contact person to facilitate resolution of requests.

IIS also recommends that AGD work with RTAs to ensure that individuals do not have to contact multiple agencies to resolve issues arising from use of face matching services. For example, AGD could coordinate a single point of contact for inquiries and resolution of match failures or could require the first agency contacted to coordinate resolution of the problem.

The approaches should be reflected in the IGA, amending legislation, Participation Agreement, NDLFRS Hosting Agreement and user guidance.

6.3.3.2 Monitoring data and matching accuracy

Awareness of actual practices on the ground, and acting to minimise impact on individuals, would be an important safeguard against transferring risks to individuals.

Recommendation 5 – Monitoring data accuracy

IIS recommends that AGD work with the NISCG to monitor and report on the frequency and nature of face matching fails arising from use of the FVS and OPOLS and the way state and territory agencies or other users handle such fails. They should take steps to identify underlying causes for the match fails and change policies or procedures as needed to minimise the impact on individuals.

6.3.4 APPs – Security

As noted in the earlier sections describing the NDLFRS, AGD and the governance bodies intend to undertake the development, implementation and ongoing operation of multifaceted privacy and security safeguards. These include Access Policies that set out the requirements that agencies and organisations must meet in order to gain and maintain access to each Face Matching Service.

IIS notes the proposed security measures and assessment processes. It does not have additional recommendations other than with respect to the retention of data.

As general principle, security risks are minimised where personal information is held only for as long as it is needed for legitimate purposes.

Minimising the retention of personal information was an important design principle for the Document Verification Service (DVS).[7] Personal information transmitted through the DVS Hub is retained no longer than 24 hours; audit logs of information transfers and some related matters are retained for review.

The NFBMC Hub similarly avoided the retention of any readily identifiable personal information. There is an audit log of Hub transactions but this does not contain any personal information.

IIS understands that AGD is still considering the data retention regime for the various elements of the NDLFRS and the Hub as follows:

- NDLFRS template store – The template store would retain only the current template of an image (as images are updated they overwrite any existing templates), however the policy in relation to templates where a licence has been cancelled or a driver is deceased is still to be decided
- Face match requests and responses – These would be destroyed immediately once the transaction is complete
- Hub and NDLFRS audit log – The Hub and NDLFRS audit data would be retained for the minimum period necessary; the current thinking is that the audit data would be kept for three months after the annual audits are completed, or a maximum of 15 months after a transaction is performed.

[7] An overview of the DVS is available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/DocumentVerificationService.aspx

IIS supports the general approach. It encourages AGD to develop these approaches into a formal data retention policy as soon as possible.

Recommendation 6 – Formal data retention policy

IIS recommends that AGD in consultation with the jurisdictions develop a data retention policy for the NDLFRS that provides for requests or queries, templates and audit logs and other related information to be retained for the minimum time possible. Unless there are good reasons for a different approach these should be similar to the DVS retention times or better.

6.3.5 APPs – Access and correction

As noted in Section 6.3.1, AGD considers that in hosting and managing the NDLFRS it would be subject to the Privacy and FOI Acts. It anticipates it would be responsible for handling requests for access or correction under these laws. However, AGD would not have direct access to personal information within the NDLFRS and so would need to work with the states and territories to respond to all such requests.

The privacy regulator meeting noted potential issues in this area. There was interest in ensuring that:

- AGD is able to provide clear advice on FOI or access and correction requests to inquirers
- States' and territories' laws, and interests in the NDLFRS data, are considered and that consistent decisions are made
- Individuals are not disadvantaged, for example by time delays or having to make requests multiple times
- AGD would be in a position to respond appropriately to potentially frivolous requests, such as for a copy of a biometric template.

AGD advises that an FOI Policy for the Face Matching Services is being developed that would outline how AGD would apply the Commonwealth FOI Act to information held in the NDLFRS. Development of the policy is being informed by a scenario-based analysis of potential FOI requests.

IIS understands a similar policy would be developed for handling access or correction requests under the Privacy Act.

IIS support this approach. Clarity on roles and processes in handling all requests for access, and for AGD's help desk staff to be able to provide well informed assistance to individuals, should minimise the risk that individuals are unable to resolve issues or exercise their rights.

Recommendation 7 – Clarity on roles and processes in responding to requests for access or other assistance

IIS recommends that AGD and Participating Agencies have detailed agreements on the handling of individual requests for access to, or correction of, driver licence information that are made to AGD as the NDLFRS manager or host.

IIS recommends that if any legal impediments to the flow of information to meet these requests be identified, suitable amending legislation be introduced by the affected jurisdiction, working closely with AGD, to ensure consistency.

IIS also recommends that AGD's NDLFRS help desk staff have instructions, based on worked out scenarios, on how to assist individuals.

6.3.6 Data breach management

Data breaches are increasingly associated with large data handling systems and information exchanges and there is no evidence that the NDLFRS would be immune.

The privacy regulators meeting saw response to data breaches as a challenging area. Questions include deciding where a breach occurred and which agency is responsible. For example, where a police agency in one state conducts a check against driver licence information held in another state or territory it could need forensic analysis to work out which instance of data was involved and which agency, and which regulator, should be responsible. The regulators also raised questions about the cost of oversight and resourcing; lack of resources is often where 'things fall apart'.

The regulators anticipated the need for cooperation in investigating some data breaches. They queried how this might work in jurisdictions without privacy laws. Given the number of interconnecting agreements, they also saw the potential for issues to fall through the cracks.

The regulators identified the need for clear protocols for investigating and responding to data breaches.

IIS agrees that this is an important issue. The IGA asks the parties to acknowledge that the Privacy Act, including the Notifiable Data Breach Scheme (which comes into effect in February 2018) will apply to personal information held in the NDLFRS. IIS understands that further detail on these arrangements will be reflected in the NDLFRS Hosting Agreement.

However, the IGA does not currently call for RTAs to notify AGD or other jurisdictions of data breaches that could affect the NDLFRS. IIS considers the IGA and/or the related NDLFRS Hosting Agreement and Participation Agreement should include clear requirements on handling data breaches. It also considers the data breach management requirements should extend to all information in the NDLFRS, not just personal information.

Recommendation 8 – Proactive and coordinated data breach management

IIS recommends that AGD work with the NISCG to ensure that the IGA, the NDLFRS Hosting Agreement and/or the Participation Agreement as appropriate, includes requirements on all participants for the notification and handling of significant data breaches that could affect the operation of the NDLFRS. The requirements should provide clarity about who would be responsible in the event of data breach and should ensure that the relevant privacy regulator and affected individuals should be notified about significant breaches in the same circumstances as in the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.

6.3.7 Benefits realisation

AGD and the jurisdictions expect that the NDLFRS would contribute to the anticipated benefits of the Face Matching Services. These include increased capability to combat identity crime as well as other law enforcement and administrative improvements (see Section 5 above).

In its response to the 2015 Preliminary PIA of the Hub – which recommended a comprehensive approach to benefits realisation – AGD indicated that it would develop a methodology to assess the costs and benefits of the Hub and Face Matching Services that includes consideration of privacy impacts and oversight costs, including costs for privacy regulators. AGD's response noted that the latter point would add to the complexity of the methodology and it would need input and agreement from all jurisdictions.

A factor in assessing benefits has been the absence of reliable statistics on identity crime. The need for reliable statistics was identified as a key priority in the Council for Australian Government's 2012 *National Identity Security Strategy*. In the last two years AGD has been funding and working with the Australian Bureau of Statistics on the Identity Crime Measurement Project. The project has identified current practices that militate against the production of sufficient, comparable statistics. The recommendations are now being considered.

AGD is now in the process of developing a benefits realisation model. IIS welcomes this. It would be desirable to have the model implemented as soon as possible.

IIS understands from the approaches so far flagged that AGD would be seeking to measure the benefits accruing to specific areas, such as fraud prevention, strengthened identity issuance and improved service delivery. If the model can also measure the contribution that different parts of the system, including the NDLFRS, make to the outcomes this would allow for a clearer assessment of the costs and benefits, including privacy benefits and costs, as incremental changes are made to the system.

The analysis should also be able to ascribe benefit accrual to particular components of the NFBMC initiative, in this instance the incremental benefit from bringing in data from RTA holdings.

Recommendation 9 – Benefits Realisation

IIS strongly support the developments of a benefits realisation model. IIS recommends that AGD ensure that the proposed model be able to identify the benefits that accrue from the NDLFRS as well as for the NFBMC as a whole.

6.4 NDLFRS Governance

The management, governance and oversight of the inter-jurisdictional data sharing arrangements are crucial to ensuring the system achieves its objectives 'while maintaining robust privacy and security safeguards'.[8]

Some participants in the privacy regulator meeting identified these issues as potentially the most complex part of the initiative. The Commonwealth's role in the process was welcomed but some in the group also noted the difficulties that can arise in COAG processes. Some also observed that in the past their jurisdiction's NISCG liaison and coordination function has been under resourced.

IIS considered the proposed governance arrangements for the NFBMC in its preliminary PIA and it made a range of recommendations in this regard. The Government has formally responded to these recommendations, accepting them in part. This PIA takes as its starting point the Government's position that the MCPEM, NISCG and the FMS AB are the appropriate governance bodies for the NFBMC. IIS has identified some areas, some of which carry over from the preliminary NFBMC PIA, where it considers privacy risks call for some strengthening of the privacy safeguards.

6.4.1 Governance Framework

The oversight and decision-making arrangements for the NFBMC, including the NDLFRS are noted above. IIS recognises and welcomes the emphasis on privacy in the arrangements, for example the IGA includes robust privacy protections as one of its objectives.

There has been a recent change in the governance arrangements that IIS considers worthy of note. The MCPEM rather than the Law Crime and Community Safety Council (LCCSC) will now exercise ministerial oversight of the Identity Matching Services, including the NDLFRS. The MCPEM will approve the Terms of Reference for the NISCG and will have responsibility for considering significant new policy matters taking account of privacy and the public interest. However, MCPEM ministers do not have direct responsibility for privacy laws, as was the case for the LCCSC that included Commonwealth, State and Territory Attorneys-General.

IIS considers there is potential for this change to affect the focus on civil liberties and privacy issues in the NFBMC and NDLFRS oversight. IIS recognises that where the subject matter is identity security, policing and emergency services the balance between these and privacy and civil liberties interests might be clearer and more accepted within the community. However, IIS considers that the privacy and social considerations for use of the NDLFRS as a data source for the NFBMC will be different if providers of human services or commercial providers join the system. In these circumstances, the question of the governance arrangements should be revisited.

IIS understands that other aspects of the governance arrangements as they affect privacy would remain; in particular, IIS presumes that the OAIC would continue to be observer on the NISCG.

[8] Recital A, IGA

OAIC advised in the privacy regulator discussions that it is happy to continue in this role and to report back to the state and territory regulators. However, particularly given the MCPEM changes, IIS sees a need for the governance processes to be well informed by privacy expertise and perspectives, including from the other jurisdictions. IIS' preliminary PIA on the NFBMC Hub recommended that the NISCG include an independent representative able to present individuals' perspectives. IIS considers the NDLFRS implementation supports the case to strengthen this aspect of the governance agreements.

IIS suggested to the privacy regulator meeting the addition of a state or territory regulator as way of adding a further privacy perspective to the discussions. The group saw value in this option. AGD noted that it is endeavouring to ensure that states and territories are represented at a jurisdictional level on the NISCG – rather than individual agency representation – but would be open to including a representative of a state and territory privacy regulator in a similar capacity to the OAIC.

Recommendation 10 – Governance body membership

IIS recommends that AGD work with the NISCG to have the NISCG membership expanded to include at least one state or territory privacy regulator in addition to the Australian Privacy Commissioner.

IIS also recommends that the question of the appropriate oversight body for the NFBMC and the NDLFRS be revisited if access to services using NDLFRS data is extended to human service organisations or commercial providers.

6.4.2 Transparency

PbD principles call for visible and transparent practices so that stakeholders can be assured that business practices and technologies are operating according to the stated promises and objectives. This principle is of added importance where for reasons including public interest, such as in the provision of driver licence information as a data source for the Face Matching Services, individuals have a reduced level of personal control over their personal information.

The NFBMC and NDLFRS governance arrangements provide for a range of transparency measures. These include the proposed legislative framework for the NFBMC, requirements in the IGA for PbD approaches including undertaking PIAs and central reporting on the use of services, including the NDLFRS.

These measures are important and welcomed. IIS identified two areas specific to the governance of the NDLFRS – publication of PIAs and reporting of NDLFRS usage – that it considers would complement and strengthen the currently proposed measures.

6.4.2.1 Publication of PIAs for NDLFRS

IIS understands that, in accordance with the PbD principle in the IGA, AGD expects RTAs would undertake PIAs relating to their use of the NDLFRS. The PIAs themselves are outside the scope of this PIA (and would be subject to any guidance, including regulator consultation and oversight, privacy regulators have issued for the jurisdiction).

IIS understands the NFBMC governance processes, including those applying to the NDLFRS, are intended to set a framework and standards, including for privacy protection measures. IIS presumes that this would include applying current best practices for PIAs. This typically includes conducting PIA processes transparently, to the extent possible, for example publishing PIA reports.[9]

While the IGA calls for independent PIAs to be conducted, including in the context of NDLFRS use, it does not specify the publication of PIA reports. IIS understands there would be requirements in data sharing agreement between agencies for PIAs and for these to be published where feasible.

AGD has indicated that it is committed to publishing PIAs. It noted that:

- The preliminary PIA on the Hub is available from AGD's website[10]
- Other PIAs in progress, including this one, would be published.

However, IIS notes that some other NFBMC participants have been cautious about publishing full PIA reports. Where summaries are published they tend to be high level. IIS recognises that there could be real security risks in publishing some details. However, as discussions with the privacy regulators identified, factors such as past practices, agency culture and the lack of privacy law in some jurisdictions, could militate against publication even where feasible.

Given the central role that PIAs are given in the privacy protection arrangements for the NFBMC, including the NDLFRS, IIS considers that more could be done to limit the discretion that Participating Agencies, including RTAs, should have in relation to PIA report publication.

Recommendation 11 – Publication of privacy impact assessments for the NDLFRS access

IIS recommends that the NISCG work with the states and territories to ensure that the requirements for transparency about privacy impact assessments be non-discretionary for Participating Agencies. Where agencies are required to undertake privacy impact assessments in order to use the NDLFRS, the privacy impact assessment reports, and the agencies' responses, should be published. The only exceptions to the publishing requirement should be on security or national security grounds. If publication of a PIA is withheld, IIS recommends that:

- These should be couched narrowly and not apply to a whole report if only some aspects are sensitive
- If the whole report, or a redacted report, cannot be published a summary of the report should be published
- If the agency is unable to publish the report it should be required to be accountable by discussing the report, and its response, with an independent body such as a privacy commissioner or ombudsman and report on the fact that this has been done.

[9] See for example, the PIA guides prepared by the NSW Information and Privacy Commission and the OAIC

[10] See https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Face-verification-service.aspx

6.4.2.2 Annual reports on use of NDLFRS for Face Matching Services and OPOLS

A related transparency measure is publicly available information about the use of NDLFRS for Face Matching Services.

The governance arrangements for the NFBMC include a range of measure to promote transparency. These include possible reporting provisions in the proposed legislation and in the IGA, which provides that ‘the Commonwealth will prepare an annual report on use of the Identity Matching Services which includes information such as: the name of entities that have accessed, or received information, by using any of the Identity Matching Services, and the particular services that each entity has used’.

In the interests of full transparency, the reports should include sufficient detail to allow readers to understand the purposes for which NDLFRS information is used. IIS has earlier highlighted the importance of effective response to face matching errors particularly in the context of the OPOLS. As a matter of accountability, IIS considers the annual reports should also include information about error rates and response timeframes.

Recommendation 12 – Annual reports on use of NDLFRS for Face Matching Services and OPOLS

IIS recommends that the AGD work with the states and territories to identify relevant information about the use of the NDLFRS for inclusion in the proposed annual report on the use of Face Matching Services. IIS recommends that, in addition to the matters outlined in the draft IGA, this should include:

- Usage of the NDLFRS as source data for the FIS, by Holding Agency and Requesting Agency, with sufficient detail to enable an understanding of the purposes for which the services are used
- Usage of the NDLFRS as source data for the FVS with sufficient detail to enable understanding of the purposes for which both government bodies and private sector organisations use the service
- Usage of the OPOLS with sufficient detail to enable understanding of the volume and nature of use
- Indicative false negative or false positive matches and how long it takes for the matters to be resolved for individuals beyond usual processing times.

6.4.3 Access to OPOLS

Until the proposed legislation to support the NFBMC is in place, the lynch pins of the privacy protections for the states and territories use of the NDLFRS and OPOLS are the IGA, Participation Agreement and access policies and the NDLFRS Hosting Agreement.

OPOLS involves the comparison of one image with a number of other images held in the NDLFRS on behalf of other jurisdictions to decide whether or not any of the images match. There is potential for matching errors resulting in inconvenience or harm to individuals particularly if they have to contact a number of jurisdictions to resolve issues.

To keep these risks within manageable levels taking account of the nature of the OPOLS, AGD is already proposing measures including that:

- User Agencies would receive a limited gallery of a very small number of the highest matching images (based on a pre-configured match threshold)
- The IGA provides that the NISCG would develop a separate access policy for both OPOLS and FRAUS based on assessed security risks. Provisions are likely to include:
    - Access limited to only available RTAs, or other agreed licencing authorities
    - Use only as part of business processes when processing licence applications, transfers and renewals
    - Compliance with interagency data sharing agreements with other participating RTAs.

IIS supports the development of access policies based on the assessed risks. It would be important to ensure risks affecting individuals are specifically taken into account. As noted earlier, the expectation is that agency 'back end' processes will investigate and resolve face match failures or discrepancies. Such processes appear likely to minimise the risks that could arise if decisions are made on match errors without human review or if individuals are expected to go to source agencies to resolve matching errors. To ensure privacy risks are not transferred to individuals, and subject to any findings in state and territory jurisdictions, there should be requirements to this effect in the OPOLS access policy.

Recommendation 13 – OPOLS Access Policy

IIS supports the framework set out in the IGA for governing access to the OPOLS. In addition to the measures proposed, and subject to state and territory PIAs, IIS recommends that all adverse decisions about licence applications, transfers and renewals should be subject to a 'human' review and review processes should be designed to minimise privacy risks, inconvenience or other impacts on individuals so that they are the same as if the processes had occurred in only one jurisdiction.

6.4.4 Privacy Assurance

The assurance arrangements for a system are an essential and important part of any privacy protection framework and they are a feature of the NFBMC governance arrangements; they include annual auditing in relation to use of Face Matching Services. In addition to annual audits required of Requesting Agencies, AGD will also commission annual audits of both the Hub and NDLFRS. It expects the first of these to be done by the OAIC.

The NISCG sets the assurance process requirements and monitors the results. Assurance processes were also of interest in the privacy regulator discussions. AGD noted that the DVS assurance program, which it considers has worked well, would inform the approach.

The privacy regulators were supportive of the general approach AGD outlined. However there was discussion about options for strengthening the monitoring and assurance processes, for example, by proactive monitoring of audit logs so that any misuse of the systems, including the NDLFRS, would come to light as soon as possible. Misuse of information from the NDLFRS could, for example, involve misuse of Face Matching Services by Requesting Agencies, or misuse of the supporting systems by AGD. As noted in the IGA 'driver licences are currently the most commonly used photographic identity document in Australia and access to these facial images is critical to maximising the benefits provided by the Face Matching Services'. Equally, continued support for the NDLFRS, which would hold images of most adult Australians, is likely to be affected if there are data breaches or misuse of the information.

IIS consider that AGD should ensure it has taken all reasonable steps to proactively detect any misuse of the NFBMC that could arise with the implementation of the NDLFRS.

AGD flagged that this could be a difficult area as appropriate use and misuse could look very similar depending on the circumstances. Privacy regulators noted that expert advice was available in this area and encouraged AGD to seek input.

Recommendation 14 – Monitoring use of NDLFRS data

IIS recommends that AGD ensure it has taken all reasonable steps to proactively detect any misuse of the NFBMC that could arise with the implementation of the NDLFRS including, to the extent practical, proactively monitoring audit logs of its use of the system to detect as soon as possible any nefarious or poor practices.

6.4.5 Privacy regulator oversight and investigations

IIS identified the importance of well-resourced independent oversight of the NFBMC in its preliminary PIA and it considers this would be increasingly important as implementation of the Face Matching Services expands and new systems such as the NDLFRS and new services such as OPOLS and FRAUS come on line. AGD's response to the PIA acknowledges that 'any legislative impediments to cross-jurisdictional cooperation and information sharing between oversight bodies may have an impact on the regulation and oversight of agencies' use of the Services. However, the oversight of cross-jurisdictional information sharing is broader than the Services and as such would be more appropriately dealt with outside of the proposed IGA'.[11]

Discussions with the privacy regulators confirmed that the need for coordinated and well-resourced response to privacy oversight and investigations remains a critical issue and that there would be some complex challenges. Issues discussed included the need for:

- Privacy regulation to reflect the multi-agency and cross-jurisdictional nature of the NDLFRS
- Processes to prevent, detect and respond to privacy issues to be clearly documented and agreed between Participating Agencies, including each agencies' role and responsibilities
- Privacy regulator cross-jurisdictional help, investigations or oversight where more than one jurisdiction is involved in a transaction and whether this could happen within current

[11] See https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/AGD-response-privacy-impact-assessment.pdf

arrangements or whether additional function or legislative powers would be needed, particularly for jurisdictions without privacy laws

- Adequate resourcing for privacy regulators.

IIS appreciates that some of these matters would be the responsibility of the states and territories but it considers that AGD and the MCPEM should be seeking to have them resolved. It notes, for example, that IGA provides that 'Each party will be responsible for any additional resourcing of privacy regulators and other oversight bodies that may be required to ensure the compliance of their respective Agencies with this Agreement'. There is currently no requirement or encouragement to ensure resourcing is adequate.

IIS considers that this issue is critical and should not be allowed to fall between the jurisdictions and left unresolved. If sufficient funding cannot be provided IIS would consider this to be a very significant failing in the privacy framework for the NDLFRS.

Recommendation 15 – Resourcing and coordination of privacy oversight and investigations

IIS recommends that AGD work with the NISCG and privacy regulators in each of the jurisdictions to ensure that mechanisms and resourcing for external oversight of RTAs sharing NDLFRS data via the Face Matching Services – by privacy regulators, Ombudsmen or anti-corruption bodies – are commensurate with data flows and that any impediments to cooperation and information sharing between oversight bodies are removed.

IIS further recommends that any legislative impediments to such cooperation and information sharing should be addressed, including via provisions in the proposed NFBMC legislation or in the IGA or other binding agreements for the use of NDLFRS services.

IIS also recommends that NDLFRS not proceed unless resourcing issues are satisfactorily addressed.

6.4.6 Review

The preliminary PIA of the Hub recommended a regular systemic review of the capability and associated arrangements. AGD supported the intent of the recommendation and the IGA provides for a review of the identity matching services to be undertaken every three years and for results to be provided to the MCPEM and published online. AGD advises that the proposed Commonwealth legislation to support the NFBMC would provide for a statutory review to commence within 5 years.

IIS welcomes both initiatives. To help ensure that the appropriate data would be available for the review to identify any privacy issues arising, to assess the effectiveness of privacy safeguards, for the NDLFRS it would be preferable if the terms of reference for the review were settled as soon as possible but at least within 12 months of the commencement of the NDLFRS. IIS considers these could address the matters raised in this PIA, including:

- The extent to which individuals are aware and comfortable with the inclusion of images in the NDLFRS
- Where use of NDLFRS data via the Face Matching Services is subject to consent, whether the consent processes used are best practice

- The number and nature of false negative or false positive errors encountered by RTAs when matching using NDLFRS data and the indicative sources of error
- Feedback from privacy regulators on any difficulties in providing effective oversight of, and privacy complaint handling arising from, RTAs' information sharing of NDLFRS data via the Face Matching Services
- Benefits actually realised for the NDLFRS.

Recommendation 16 – Review of the operation of the NDLFRS

IIS recommends that as soon as possible after the NDLFRS goes live, AGD work with the NISCG, RTAs and jurisdiction privacy regulators to develop terms of reference for the proposed three-year review of the Identity matching services to ensure that issues relevant to the privacy impacts of the NDLFRS are included. The review criteria should take account of matters raised in this PIA and in further PIAs on agency, jurisdiction or private sector use of data within the NDLFRS, including:

- The extent to which individual are aware and comfortable with the inclusion of images in the NDLFRS
- Where use of NDLFRS data via the Face Matching Services is subject to consent, whether the consent processes used are best practice
- The number of nature of false negative or false positive errors RTAs encounter in matching using NDLFRS data and the indicatives sources of error
- Feedback from privacy regulators on any difficulties in providing effective oversight of, and privacy complaint handling arising from, RTAs' information sharing of NDLFRS data via the Face Matching Services
- Benefit actually realised for the NDLFRS

The NISCG should ensure that AGD, RTAs and other NDLFRS users have systems in place to collect the information for the review based on the terms of reference.

6.5 Other issues

6.5.1 Legal framework

The proposed legal framework to support the NFBMC, including the NDLFRS, is outside of the scope of this PIA. The Australian Government Solicitor (AGS) is undertaking a PIA on the proposed Commonwealth legislation.

The proposed legislation was discussed in the privacy regulator consultations and the regulators were invited to provide feedback to AGS. However, some issues were raised in the discussions that IIS considers are important to note here. These were as follows:

- Ability of states and territories to share information with jurisdictions without privacy laws, particularly given the cross-border data flow provisions in some privacy laws
- How to ensure that in providing information to another jurisdiction there would be proper privacy and security systems to ensure that the data is protected end-to-end

- The oversight and privacy complaint processes for jurisdictions without privacy laws and to make enforcement in these circumstances more than via informal agreements.

From the information and discussions to date IIS understands that there will be legally binding mechanisms available, with privacy and security obligations, to authorise disclosures of information to jurisdictions without privacy laws. However, it is less clear that there would be effective redress channels for individuals if information is mishandled. IIS considers that the issues raised point to potential gaps in privacy safeguards. It suggests that an approach such as contained in APP 8.2 be built into the proposed legislation.

Recommendation 17 – Gaps in privacy safeguards where jurisdictions do not have privacy law

IIS recommends that the proposed Commonwealth legislation to support the NFBMC require that agencies or organisations seeking access to Face Matching Services relying on the NDLFRS be subject to a law, or binding scheme, that has the effect of protecting personal information used in face matching services in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information and that there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme.

6.5.2 Governance of change

IIS identified the governance of change, and particularly which bodies make decisions on how the system evolves, as a privacy risk area in its preliminary PIA on the NFBMC Interoperability Hub. It also sees this area as important to the privacy impacts of the NDLFRS.

The discussions with privacy regulators indicated that a change to the NDLFRS scope, particularly around new services or User Agencies for the FIS, is a key issue.

AGD indicated that any major changes would require approval by the NISCG and then MCPEM. Depending on the nature of the change, a regulation may also be required pursuant to the proposed Commonwealth legislation.

AGD also raised for discussion the scope and number of PIAs that might be undertaken as the next phase of the NDLFRS implementation proceeds. The group strongly supported AGD's preference for joined-up assessments covering groups of similar agencies. AGD indicated that it intends on working with Austroads to undertake a PIA covering state and territory RTA use of the Face Matching Services against the different data sources. There are plans for a similar PIA covering law enforcement use. To the fullest extent possible, AGD intends on making all PIAs and the government responses publicly available.

IIS also supports the suggested 'joined up' approach provided that this does not limit the opportunity for a range of independent views on privacy to be brought to the table. In general, IIS considers that significant changes to the NDLFRS (and the NFBMC more broadly) should be conducted transparently and with input from a range of privacy perspectives. The processes should at least involve consultation with state and territory privacy regulators and preferably also with community representatives.

Recommendation 18 – Changes to NDLFRS

IIS supports AGD's view that the governance arrangements for the NDLFRS should ensure that significant changes to the Face Matching Services relying on the NDLFRS such as new types services, new purposes or new categories of users are subject to privacy impact assessments. IIS recommends that such significant changes should also be subject to consultation with privacy regulators in all jurisdictions and with community representatives.

7. Appendix A – Table of recommendations

	Recommendation Title	Recommendation
Operation **APPs**	**Recommendation 1 – Ensuring RTAs control NDLFRS information and individual rights are maintained**	IIS recommends that AGD ensure that: ● Any changes to the NDLFRS administrative or legal arrangement that could affect the extent to which the states and territories remain in control of information in their partitions of the NDLFRS should be subject to a transparent PIA process ● The application of privacy and FOI law to NDLFRS data in AGD hands, including the respective roles and responsibilities for the Commonwealth and states and territories, should be clarified in law or in the IGA and legally binding participation and/or hosting agreements ● Individuals are not disadvantaged by any inadvertent impacts of the legal provisions or administrative approach, for example, on individuals' right to pursue a privacy complaint under a state or territory privacy law.
Operation **APPs** **Collection, use and disclosure**	**Recommendation 2 – Transparency and information for individuals**	IIS recommends that AGD work with the NISCG and participating organisations to ensure that the IGA or the NDLFRS Hosting Agreement include non-discretionary requirements for RTAs to provide explicit up-front notice to future driver licence applicants about the Commonwealth's collection of driver licence images for biometric face matching for law enforcement, national security and other purposes. In addition, IIS recommends that either AGD or RTAs take proactive steps to notify individuals whose information is already held by RTAs about the inclusion of their information in the NDLFRS. This could involve mail-outs to individuals and/or a public education campaign. IIS also recommends that AGD develop and disseminate information, for example in its privacy policy, and via its website, or brochures distributed by RTAs, that provides specific details on the information that would be collected for the NDLFRS and how it stored and used and the associated privacy safeguards. Information about how individuals can seek help to resolve any identity problems arising as a result of use of the NDLFRS should be included.
Operation **APPs** **Collection,**	**Recommendation 3 – Requirements for consent based access to NDLFRS**	IIS recommends that AGD work with the NISCG and Participating Agencies to ensure that where organisations are permitted to use the FVS to access facial images from the NDLFRS on the basis that individuals have given their consent:

	Recommendation Title	Recommendation
use and disclosure		- The consent must be express, freely given and fully informed - Consistent with the Commonwealth Digital Service Standard, there must be a viable alternative method available for individuals to authenticate or verify their identity - This requirement is included in the proposed legislation for the NFBMC.
Operation APPs **Accuracy**	**Recommendation 4 – Process to handle false negative matches**	IIS recommends that AGD work with Road Transport Agencies to develop a strong privacy approach to the handling of ‘no match’ or error responses following a face match request using the NDLFRS by doing such things as: - Undertaking risk assessments to identify issues that might arise for individuals - Encouraging consistent business processes across all jurisdictions - Identifying agreed benchmarks for resolving issues and ensuring resources are available to meet the benchmarks - Requiring each jurisdiction to have resources available to resolve issues for their own customers and to respond to requests from other jurisdictions within a reasonable time frame. Each jurisdiction should also provide up-to-date details for a contact person to facilitate resolution of requests. IIS also recommends that AGD work with RTAs to ensure that individuals do not have to contact multiple agencies to resolve issues arising from use of face matching services. For example, AGD could coordinate a single point of contact for inquiries and resolution of match failures or could require the first agency contacted to coordinate resolution of the problem. The approaches should be reflected in the IGA, amending legislation, Participation Agreement, NDLFRS Hosting Agreement and user guidance.
Operation APPs **Accuracy**	**Recommendation 5 – Monitoring data accuracy and matching processes**	IIS recommends that AGD work with the NISCG to monitor and report on the frequency and nature of face matching fails arising from use of the FVS and OPOLS and the way state and territory agencies or other users handle such fails. They should take steps to identify underlying causes for the match fails and change policies or procedures as needed to minimise the impact on individuals.

	Recommendation Title	Recommendation
Operations **APPs** **Security**	**Recommendation 6 – Formal data retention policy**	IIS recommends that AGD in consultation with the jurisdictions develop a data retention policy for the NDLFRS that provides for requests or queries, templates and audit logs and other related information to be retained for the minimum time possible. Unless there are good reasons for a different approach these should be similar to the DVS retention times or better.
Operations **APPs** **Access and correction**	**Recommendation 7 – Clarity on roles and processes in responding to requests for access to information**	IIS recommends that AGD and Participating Agencies have detailed agreements on the handling of individual requests for access to, or correction of, driver licence information that are made to AGD as the NDLFRS manager or host. IIS recommends that if any legal impediments to the flow of information to meet these requests be identified, suitable amending legislation be introduced by the affected jurisdiction, working closely with AGD, to ensure consistency. IIS also recommends that AGD's NDLFRS help desk staff have instructions, based on worked out scenarios, on how to assist individuals.
Operations **Data breach management**	**Recommendation 8 – Proactive and coordinated data breach management**	IIS recommends that AGD work with the NISCG to ensure that the IGA, the NDLFRS Hosting Agreement and/or the Participation Agreement as appropriate, includes requirements on all participants for the notification and handling of significant data breaches that could affect the operation of the NDLFRS. The requirements should provide clarity about who would be responsible in the event of data breach and should ensure that the relevant privacy regulator and affected individuals should be notified about significant breaches in the same circumstances as in the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.
Operations **Benefits realisation**	**Recommendation 9 – Benefits realisation**	IIS strongly support the developments of a benefits realisation model. IIS recommends that AGD ensure that the proposed model be able to identify the benefits that accrue from the NDLFRS as well as for the NFBMC as a whole.
Governance Framework	**Recommendation 10 – Governance body membership**	IIS recommends that AGD work with the NISCG to have the NISCG membership expanded to include at least one state or territory privacy regulator in addition to the Australian Privacy Commissioner. IIS also recommends that the question of the appropriate oversight body for the NFBMC and the NDLFRS be revisited if access to services using NDLFRS data is extended to human service organisations or commercial providers.

	Recommendation Title	Recommendation
Governance **Transparency**	**Recommendation 11 – Publication of privacy impact assessments for the NDLFRS access**	IIS recommends that the NISCG work with the states and territories to ensure that the requirements for transparency about privacy impact assessments be non-discretionary for Participating Agencies. Where agencies are required to undertake privacy impact assessments in order to use the NDLFRS, the privacy impact assessment reports, and the agencies' responses, should be published. The only exceptions to the publishing requirement should be on security or national security grounds. If publication of a PIA is withheld, IIS recommends that: ● These should be couched narrowly and not apply to a whole report if only some aspects are sensitive ● If the whole report, or a redacted report, cannot be published a summary of the report should be published ● If the agency is unable to publish the report it should be required to be accountable by discussing the report, and its response, with an independent body such as a privacy commissioner or ombudsman and report on the fact that this has been done.
Governance **Transparency**	**Recommendation 12 – Annual reports on use of NDLFRS for Face Matching Services and OPOLS**	IIS recommends that the AGD work with the states and territories to identify relevant information about the use of the NDLFRS for inclusion in the proposed annual report on the use of Face Matching Services. IIS recommends that, in addition to the matters outlined in the draft IGA, this should include: ● Usage of the NDLFRS as source data for the FIS, by Holding Agency and Requesting Agency, with sufficient detail to enable an understanding of the purposes for which the services are used ● Usage of the NDLFRS as source data for the FVS with sufficient detail to enable understanding of the purposes for which both government bodies and private sector organisations use the service ● Usage of the OPOLS with sufficient detail to enable understanding of the volume and nature of use ● Indicative false negative or false positive matches and how long it takes for the matters to be resolved for individuals beyond usual processing times.
Governance **Access**	**Recommendation 13 – OPOLS Access Policy**	IIS supports the framework set out in the IGA for governing access to the OPOLS. In addition to the measures proposed, and subject to state and territory PIAs, IIS recommends that all adverse decisions about licence applications, transfers and renewals should be subject to a 'human' review and review

	Recommendation Title	Recommendation
policies		processes should be designed to minimise privacy risks, inconvenience or other impacts on individuals so that they are the same as if the processes had occurred in only one jurisdiction.
Governance **Privacy Assurance**	**Recommendation 14 – Monitoring use of NDLFRS data**	IIS recommends that AGD ensure it has taken all reasonable steps to proactively detect any misuse of the NFBMC that could arise with the implementation of the NDLFRS including, to the extent practical, proactively monitoring audit logs of its use of the system to detect as soon as possible any nefarious or poor practices.
Governance **Oversight and investigations**	**Recommendation 15 – Seamless privacy oversight and investigations**	IIS recommends that AGD work with the NISCG and privacy regulators in each of the jurisdictions to ensure that mechanisms and resourcing for external oversight of RTAs sharing NDLFRS data via the Face Matching Services – by privacy regulators, Ombudsmen or anti-corruption bodies – are commensurate with data flows and that any impediments to cooperation and information sharing between oversight bodies are removed. IIS further recommends that any legislative impediments to such cooperation and information sharing should be addressed, including via provisions in the proposed NFBMC legislation or in the IGA or other binding agreements for the use of NDLFRS services. IIS also recommends that NDLFRS not proceed unless resourcing issues are satisfactorily addressed.
Governance **Review**	**Recommendation 16 – Review of the operation of the NDLFRS**	IIS recommends that as soon as possible after the NDLFRS goes live, AGD work with the NISCG, RTAs and jurisdiction privacy regulators to develop terms of reference for the proposed three-year review of the Identity matching services to ensure that issues relevant to the privacy impacts of the NDLFRS are included. The review criteria should take account of matters raised in this PIA and in further PIAs on agency, jurisdiction or private sector use of data within the NDLFRS, including: ● The extent to which individual are aware and comfortable with the inclusion of images in the NDLFRS ● Where use of NDLFRS data via the Face Matching Services is subject to consent, whether the consent processes used are best practice ● The number of nature of false negative or false positive errors RTAs encounter in matching using NDLFRS data and the indicatives sources of error ● Feedback from privacy regulators on any difficulties in providing effective oversight of, and privacy complaint handling arising from, RTAs' information sharing of NDLFRS data via the Face Matching Services

	Recommendation Title	Recommendation
		- Benefit actually realised for the NDLFRS The NISCG should ensure that AGD, RTAs and other NDLFRS users have systems in place to collect the information for the review based on the terms of reference.
Legal framework	**Recommendation 17 – Gaps in privacy safeguards where jurisdictions do not have privacy law**	IIS recommends that the proposed Commonwealth legislation to support the NFBMC require that agencies or organisations seeking access to Face Matching Services relying on the NDLFRS be subject to a law, or binding scheme, that has the effect of protecting personal information used in face matching services in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information and that there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme.
Governance **Change**	**Recommendation 18 – Changes to NDLFRS**	IIS supports AGD’s view that the governance arrangements for the NDLFRS should ensure that significant changes to the Face Matching Services relying on the NDLFRS such as new types services, new purposes or new categories of users are subject to privacy impact assessments. IIS recommends that such significant changes should also be subject to consultation with privacy regulators in all jurisdictions and with community representatives.

8. Appendix B – Scope, deliverables and methodology

8.1 Methodology

IIS undertook the following steps in completing this PIA:

- Planning – IIS finalised its work plan following discussions with AGD on matters including project objectives, stakeholders, key tasks and milestones
- Information gathering – IIS gathered and read material and held meetings to gain a sufficient understanding of AGD's thinking, research and work to date on the NDLFRS system – including elements of the system, technical requirements, stakeholders, potential data flows and possible risks – to inform its analysis and recommendations
- Analysis – IIS analysed the material gathered taking account of the specified information flows within the NDLFRS
- Drafting and finalising reports

8.2 Documents reviewed and meetings held

Documents Reviewed
1. AGD and ABS Identity Crime measurement project – Summary paper
2. Austroads Business Case – National Driver Licence Facial Recognition Solution
3. Benefits Realisation Model – Interoperability Hub – Ideas and Approaches
4. Business Case Elements – NSW Participation in the NDLFRS – draft July 2017
5. Data Gateway Service – Technical Concept of Operations
6. Face Identification Access Policy – Final 21 June 2017
7. Face Match Service Advisory Board Terms of Reference Draft
8. Face Matching Services – Implementation Update – May 2017
9. Face Verification Service Access Policy – Final 22 June 2017
10. Fact Sheet – National Facial Biometric Matching Capability
11. Identity Crime Infographic
12. Identity Security - Identity Crime Measurement project – Phase 3 Final Report
13. Multilateral IGA - Version 2 - May 2017
14. National Identity Security Coordination Group Terms of Reference Draft
15. National Privacy Commissioners Forum – draft minutes 3 August 2017
16. NDLFRS – Simple Architecture Design Presentation – December 2015
17. NFBMC and NDLFRS – Overview for National Privacy Commissioner Forum

Documents Reviewed
18. NFBMC Face Verification Service Template Interagency Data Sharing Arrangement
19. NFBMC Hub and Spoke Architecture
20. NFBMC Privacy Safeguards Overview
21. Privacy Safeguards – Overview for the National Privacy Commissioner Forum
22. Proposed legislation to support the National Facial Biometric Matching Capability – paper for the National Privacy Commissioner Forum
23. State and Territory Legal Issues 2017 – Item 5 – Discussion paper

Meetings	Date	Participants
AGD	6 July 2017	Various from National Facial Biometric Matching Capability, Identity and Protective Security Branch
National Privacy Forum	3 August 2017	Various from OAIC and from privacy regulators or equivalents in each of the states and territories
Road Transport Agencies	15 August 2017	Various from RTA in each of the states and territories

9. Appendix C – Summary of stakeholder issues raised in consultations and further submissions

9.1 Stakeholders consulted

Consultation meetings	Additional submissions
Privacy Regulators	
Information and Privacy Commission New South Wales	✓
Information Commissioner Northern Territory	✓
Information Commissioner Western Australia	
Office of the Australian Information Commissioner	✓
Office of the Information Commissioner Queensland	✓
Office of the Victorian Information Commissioner (previously the Commissioner for Privacy and Data Protection)	✓
Ombudsman Tasmania	
Privacy Committee of South Australia	
RTAs	
Department of Infrastructure, Planning and Logistics – Northern Territory	
Department of Justice and Community Safety and Access Canberra – Australian Capital Territory	
Department of Planning, Transport and Infrastructure – South Australia	
Department of Transport – Western Australia	✓
Department of Transport and Main Roads – Queensland	✓
Roads and Maritime Services – New South Wales	✓
State Growth Tasmania	
VicRoads	✓

9.2 Privacy regulator issues

9.2.1 Issues raised in stakeholder meeting

The group saw some strong positives in the NFBMC, including the NDLFRS, as outlined by AGD. In particular, some in the group strongly supported the potential for the NDLFRS to help prevent identity crime and to assist affected individuals to recover their compromised identity.

There was also support for the AGD's approach to implementation of the systems. The group noted the proposed measures for controlled and monitored use of the Face Matching Services, including the proposed legally binding agreements. There were also comments to the effect that there has been 'some solid work on privacy'.

The group identified a number of areas where there were still questions about privacy or management processes. In summary, these were as follows:

Limits on use and disclosure of facial image matching

There was strong support for the concept of defining, and limiting, the organisations and purposes for which NDLFRS images could be used. The permitted purposes would preferably be defined in the proposed Commonwealth legislation, but should at least be in the formal agreements governing participation. Without clear definitions as a basis for access restrictions, particularly to the more risky one-to-many Face Identification Service, there might be many state agencies that could, for example, be considered law enforcement agencies.

The group remained keen to have the opportunity to provide comments on the access policies and draft legislation. Reasonable time for consultation, for example, on the definition of 'community safety' would be needed.

Authority for disclosures between jurisdictions

Some states and territories had identified possible legal barriers to state and territory agencies using the NDLFRS to exchange images and other details arising from privacy or other laws, or lack of privacy laws (in particular, Western Australia and South Australia).

The meeting recognised this as an issue that needed to be resolved. Some regulators saw a need, in addition to the proposed Commonwealth legislation, for jurisdiction specific legislation, in part because this would provide a clearer authorisation and more transparency for individuals whose images are already held.

Other issues where jurisdictions do not have privacy laws

In addition to authority to collect or disclose information there were other possible issues identified in dealing with jurisdictions without privacy legislation. These were:

- Compliance with cross-border privacy principles embedded in state and territory privacy legislation, which usually require a substantially similar privacy law or another equivalent protection for citizen's information. An option would be provisions in legally binding agreements. This approach has been used in other Australian inter-jurisdictional information sharing arrangements, for example the current NEVDIS agreement.[12] However, some deficiencies were noted

- The mechanisms for responding to data breaches that affect multiple agencies
- Ensuring that individuals have effective redress mechanisms where there are privacy or other problems
- Whether there would be effective oversight the handling of information and enforceable sanctions in the event of mishandling of personal information.

Agencies not subject to privacy laws

Some law enforcement and national security agencies, for example, the Australian Security Intelligence Organisation and the Australian Criminal Intelligence Commission are completely exempt from the Privacy Act. The meeting noted that the IGA and access policies treat these organisations differently, for example, they are not required to complete and publish privacy impact assessments. Rather, they are required to provide a statement outlining their privacy controls around the collection, use and disclosure of sensitive personal information.

Ability for privacy regulators to investigate and cooperate an issue

The group identified that the multi-agency and cross-jurisdictional nature of the NDLFRS called for a similar approach for privacy regulation. Questions raised included whether the regulators would be able to seek or provide cross-jurisdictional help in investigations and oversight. This might occur informally but formal powers, including in relation to data exchanges, would need to be considered.

Resources available to privacy regulators could also be an impediment to effective investigations and oversight.

Data breach

The management of data breaches was identified as a challenge. Issues included:

- Identifying the source of a breach and which jurisdiction and entity would be responsible
- Resources for regulator oversight and investigations
- Ability for regulators to be able to share resources and to cooperate
- Steps to ensure regulators become aware of data breaches affecting individuals in their jurisdictions.

[12] Austroads host the National Exchange of Vehicle and Driver Information System (NEVDIS), which is a national system that exchanges information about vehicles and driver licences – see http://www.austroads.com.au/drivers-vehicles/nevdis.

Consent

The meeting discussed the conditions needed for valid consent. Most agreed that if access to data within the NDLFRS were to be authorised where individuals have consented, for example via the FVS, consent processes would need to be done well. Some suggested this would include there being a viable alternative if individuals chose not to have their identity verified using data within the NDLFRS.

Governance arrangements

There was considerable discussion about governance arrangements. Matters identified included:

- The contents of the IGA and other agreements – provisions for example in relation to PIAs, should be non-discretionary to the extent possible – and maintaining good governance into the future
- Roles and responsibilities for the Commonwealth and RTAs with respect to handling freedom of information, access or correction requests
- The potential, because number of interconnecting agreements, for issues to fall between PIA and other processes
- Possible difficulties, given experience with Council of Australian Government (COAG) coordination on privacy and freedom of information issues, in getting appropriate privacy protections – the NISCG was considered likely to play a useful role if it is properly supported and resourced
- Risks if insufficient resources are provided to RTAs or other agency users and that as a result they have difficulty in providing or continuing to provide the necessary public information, staff training, audit and risk management.

Access by private sector organisations and management of change

There was some discussion of the possible expansion of access to the NDLFRS and of expansions in the use of face recognition more generally. Issues noted included:

- The proposed governance of changes seems good but would need to be properly resourced
- Interest in seeing PIAs as changes are considered
- Potential for ‘function creep’ – that is new types of uses beyond what is currently planned. For example, face recognition and video surveillance are increasingly being considered by some local councils and private sector organisations
- The difficulty in ensuring that consent if sought met legal requirements, including availability of viable alternatives to using data within the NDLFRS
- Other possible risks in expansion, for example, some private sector organisations might not have strong security standards.

9.2.2 Key comments on draft PIA

Five of the privacy regulators provided further submissions in response to the draft PIA. Comments included suggestions for additional information or to make it easier to assess risks. IIS has amended the PIA to accommodate these comments where possible. Some comments raised issues that were out of scope for the PIA.

More substantive comments made or issues raised included:

- Support for a whole of system PIA to be conducted as soon as possible and for a holistic security risk assessment to be undertaken as well
- Difficulty in assessing privacy risks given that the legislative framework is still being developed and it is unclear at this stage what types of personal and/or sensitive information, as defined in the Privacy Act, will be included in the definition of ‘identity information’
- The necessity for inclusion of some items in the NDLFRS, for example, whether the individual wears glasses
- Need for further information/clarification on metadata and audit processes
- Need for further information/analysis about the security features of the partitioned databases
- The role and responsibilities of the private sector provider
- Aspects of the notice and consent discussion, including circumstances when agencies could not meet consent requirements, and the possible need for proactive notification for existing driver licence holdings
- Governance arrangements, including change to MCPEM as the body exercising ministerial oversight and aspects of NDLFRS audits
- Publication of PIAs including possible additional definitions or guidance on national security, or security, limitations on publishing
- Arrangements for privacy regulator resourcing and information exchange
- Processes to address gaps in privacy protections for States without equivalent privacy protections, and the effectiveness of options proposed in the PIA
- Concern about potential for scope creep, for example recent media mentions of use of real time face recognition.

9.3 Road agency issues

9.3.1 Issues raised in stakeholder meeting

The RTA group was generally supportive of the NDLFRS approaches. No insoluble privacy issues were identified. The group thought most citizens probably already expect images to be shared although they might not be aware of the specific details.

The main issues raised in discussions were:

- The possible need for additional resources to ensure management and auditing obligations are met
- Ensuring back end resolution processes and governance are in place and working well

- The potential for inconsistent business processes in each state and territory leading to inefficient management of issues or vulnerabilities in identity security – the group saw a need for discussions to ensure business process consistency and that resources and up-to-date contact details are available to respond to requests.

9.3.2 Key comments on draft PIA

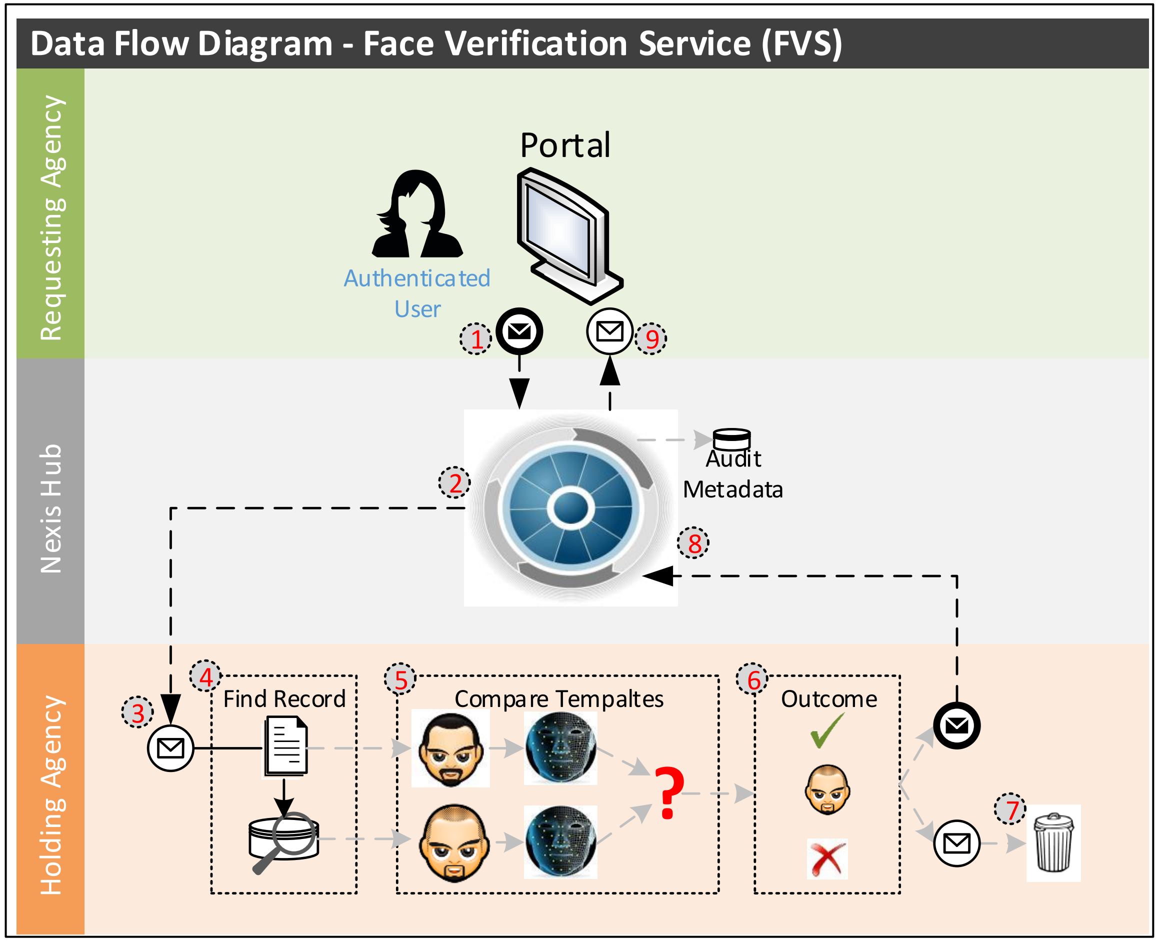
Four of the RTAs provided further submissions in response to the draft PIA. Comments included requests for clarification of terminology and aspects of the description of the NDLFRS. IIS has amended the PIA to accommodate these comments where possible. Some comments raised issues that were out of scope for the PIA.

More substantive comments made or issues raised included:

- Requests for clarification of some process issues including timeframe for NDLFRS review, participation arrangements, proposed legislation, possible future use of NDLFRS information and data quality standards
- The necessity for inclusion of some items in the NDLFRS, for example, whether the individual wears glasses, the type of vehicle driven and date of birth
- The circumstances in which consent might be required and whether alternative channels need be provided. The NSW RTA in particular noted that it had legal advice to the effect that a lack of an alternative channel would not affect the validity of any consent sought. It also noted that in the context of driver licencing, consent was not needed for identity checks to be conducted
- The possible difficulty on providing privacy notices to individuals whose information the RTA already holds
- Concern about requirements to publish PIAs; some considered a PIA to be confidential advice to the agency.

10. Appendix D – Detailed description of data flows for FVS, FIS and OPOLS

10.1 FVS



			Data			
#	Description	Notes	Inputs[13]	Transformations / Processes	Outputs	Audit
1	An Authenticated User submits a query to NEXIS Hub via the Portal, against a single Data Holding Agency. The request is encrypted upon submission.	The NEXIS Hub will capture portal metadata for the request	• Data Source • Facial Image • Document ID • Biographic Details ○ Surname ○ Given Name ○ DoB	Basic data entry validations are performed.	• Data Source • Facial Image • Document ID • Biographic Details ○ Surname ○ Given Name ○ DoB • System Username • Transaction Group ID • Transaction ID • Request Priority • Username • Requesting Agency • Match Threshold • Privilege Indicators[14]	**User activity** An audit record is created to indicate the User has submitted an FVS transaction with the following information: • Date/Time • Audit Type (e.g. User submitted an FVS Search request to <Data Source> • Username • Transaction ID **Transaction** An audit record of the transaction

[13] The user input values change subtly depending on the type of FVS transaction (Retrieve, Match, or Search)

[14] Privilege indicators reflect the privileges assigned to the User's role which allow them to view (or not) specific pieces of information as agreed between the requesting and holding agency. Indicators advise the holding agency what information is to be returned in a response. Typically privileges are: IncludeImages, IncludeBiographic, and IncludeAliases. Holding Agencies may have specific privileges for agency-specific data such as IncludeTravelDocument.

				Data		
						record is created:[15] • **Date/Time** • **Function** • **Requesting Agency** • **Username** • **System Name** • **Transaction Group ID** • **Transaction ID** • **Data Source** • Message Status • Message State • Message • **Transaction Status** • **Probe MD5#** • Response MD5#
2	The NEXIS Hub receipts, validates, and authenticates the request. Once authenticated, the request is routed to the holding agency for processing.	The NEXIS Hub will capture audit metadata for the request.	• Data Source • Facial Image • Document ID • Biographic Details	Validations occur • to verify the system user has the correct security	• Data Source • Facial Image • Document ID • Biographic Details	**Transaction** The transaction audit record is updated • **Date/Time**

[15] This is the full set of audit for an FVS transaction. Different attributes will be added/updated at various times during the audit lifecycle. Items in **bold** are those populated/updated at this step.

			Data		
		○ Surname ○ Given Name ○ DoB - System Username - Transaction Group ID - Transaction ID - Request Priority - Username - Requesting Agency - Match Threshold - Privilege Indicators	privileges to submit this transaction. - To verify the role assigned to the User allows them to submit the transaction type against the data source - To verify/determine the data privileges of the User. - Against some data attributes (such as ensuring DoB values are in correct formats).	○ Surname ○ Given Name ○ DoB - System Username - Transaction Group ID - Transaction ID - Request Priority - Username - Requesting Agency - Match Threshold - Privilege Indicators	- Function - Requesting Agency - Username - System Name - Transaction Group ID - Transaction ID - Data Source - Message Status - Message State - Message - **Transaction Status** - Probe MD5# - Response MD5#
3	The Holding Agency receipts, validates, and authenticates the request.	- Data Source - Facial Image - Document ID - Biographic Details ○ Surname ○ Given Name	This is up to each Holding Agency, however typically they: - Ensuring the request is valid;	This is up to each holding agency and how they have implemented their FVS services.	This is up to each holding agency and how they have implemented audit of their FVS services.

			Data		
			○ DoB • System Username • Transaction Group ID • Transaction ID • Request Priority • Username • Requesting Agency • Match Threshold • Privilege Indicators	and • Verifying information / attributes within the request.	
4	The Holding Agency locates the specified document for verification. If a single document is found, the image associated with that document is used for biometric comparison. If a single document cannot be found, a no match response is sent back to the Authenticated User.		This is up to each holding agency and how they have implemented their FVS services.		This is up to each holding agency and how they have implemented audit of their FVS services.
5	The Probe Image and document image are templated and compare to see if they are considered a match at or above the Holding Agencies' match threshold.		This is up to each holding agency and how they have implemented their FVS services.		This is up to each holding agency and how they have implemented audit of their FVS services.
6	Where there is a match above threshold, a Match/No Match response is generated. Where authorised, additional information (image, biographic details) may also be sent		This is up to each holding agency and how they have implemented their FVS services.		This is up to each holding agency and how they have implemented audit

				Data		
	in the response.					of their FVS services.
7	Once processed, the request is discarded.		This is up to each holding agency and how they have implemented their FVS services.			This is up to each holding agency and how they have implemented audit of their FVS services.
8	The NEXIS Hub receipts, validates, and authenticates the response. Once authenticated, the response is routed to the Authenticated user.	The NEXIS Hub will capture audit metadata for the Response.	Information returned from the data source[16] • Transaction ID • Request Priority • Match/No Match Indicator • Match Score • Document ID • Document Type • Document Status • Customer ID • Surname • GivenNames • Gender • DateofBirth • Deceased Indicator	Validations occur • to verify the system user has the correct security privileges to submit this transaction response, and • To verify the recipient of the transaction response;	• Transaction ID • Request Priority • Match/No Match Indicator • Match Score • Document ID • Document Type • Document Status • Customer ID • Surname • GivenNames • Gender • DateofBirth • Deceased Indicator • Message • Message State	**Transaction** The transaction audit record is updated • **Date/Time** • Function • Requesting Agency • Username • System Name • Transaction Group ID • Transaction ID • Data Source • **Message Status** • **Message State**

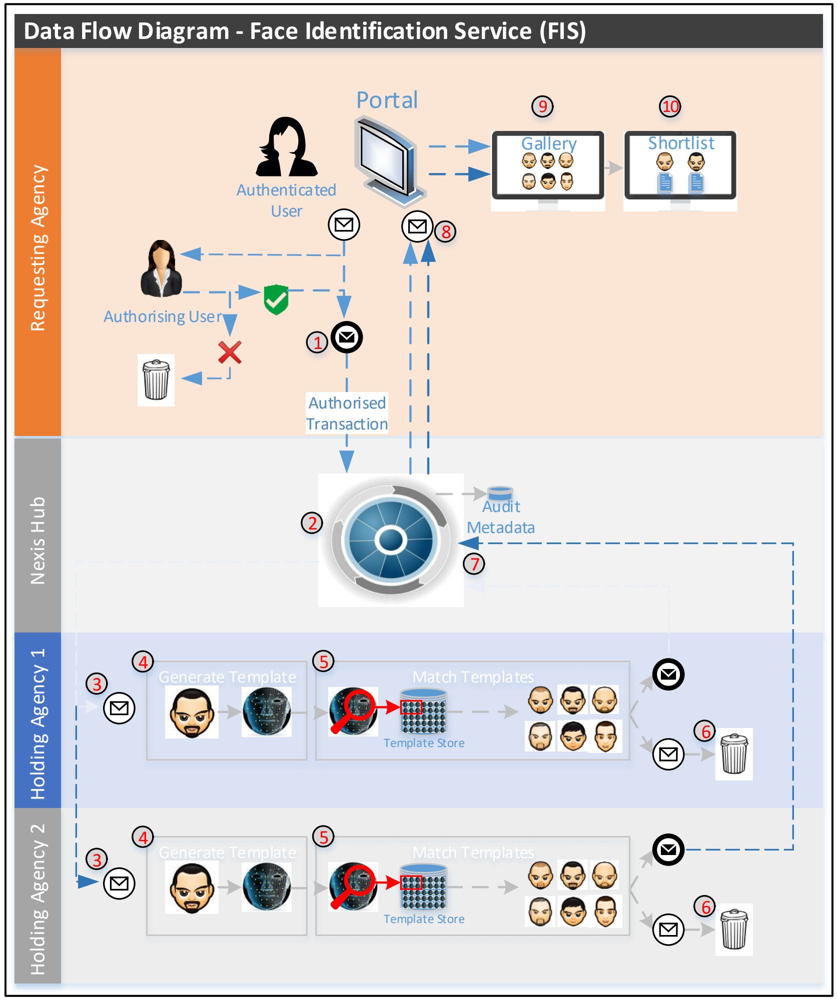
[16] While there are common elements of information that may returned from each holding agency, there are also specific data elements. Specific elements have not been captured here in detail.

The attributes listed here are the generic ‘full’ set of elements that may be returned. The Privilege Indicators sent in the request will mean that some elements may not be returned (again, depending on the agreed roles between the Requesting and Holding Agencies).

			Data		
			• Message • Message State • MessageStatusCode • Data-source specific attributes	• MessageStatusCode	• **Message** • **Transaction Status** • Probe MD5# • **Response MD5#**
9	The Authenticated User is able to view the response from the Data Holding Agency to resolve their verification query. Once viewed the result is discarded by the Portal and cannot be re-viewed.	The NEXIS Hub will capture portal metadata for the response	• Transaction ID • Request Priority • Match/No Match Indicator • Match Score • Document ID • Document Type • Document Status • Customer ID • Surname • GivenNames • Gender • DateofBirth • Deceased Indicator • Message • Message State • MessageStatusCode		**User activity** An audit record is created to indicate the User has viewed the FVS transaction with the following information: • Date/Time • Audit Type (e.g. User viewed the FVS Search response to <Data Source> • Username • Transaction ID **Transaction** The transaction audit record is updated • **Date/Time** • Function

Data
• Requesting Agency • Username • System Name • Transaction Group ID • Transaction ID • Data Source • Message Status • Message State • Message • **Transaction Status** • Probe MD5# • Response MD5#

10.2 FIS


Data Flow Diagram - Face Identification Service (FIS)
Requesting Agency
Portal
9
10
Gallery
Shortlist
Authenticated User
8
Authorising User
1
Authorised Transaction
Nexis Hub
2
Audit Metadata
7
Holding Agency 1
3
4
Generate Template
5
Match Templates
Template Store
6
Holding Agency 2
3
4
Generate Template
5
Match Templates
Template Store
6

Data

				Data		
#	Description	Notes	Inputs	Transformations / Processes	Outputs	Audit
1	An Authenticated User submits a query to NEXIS Hub via the Portal, against a one or several Data Holding Agencies. The request is encrypted upon submission. In some instances the request will first require authorization before being sent to Holding Agencies for processing.		• Data Sources • Facial Image • Gender • Purpose • Category • Subject[17] • Act • Section • Supervising Officer • Authorising Officer[18] *For each selected data source[19]* • Age Range • Number of records to be returned • Match threshold • Priority	Basic data entry validations are performed.	• Data Sources • Facial Image • Gender • Purpose • Category • Subject • Act • Section • Supervising Officer • Authorising Officer *For each selected data source* • Age Range • Number of records to be returned • Match threshold • Priority	**User activity** An audit record is created to indicate the User has submitted an FVS transaction with the following information: • Date/Time • Audit Type (e.g. User submitted an FIS Identify request to <Data Source 1>, <Data Source 2> ... and <Data Source X>)

[17] Purpose, Act, & Section are populated based upon pre-defined lists the user selects from.

[18] Authorising Officers are only required where specific criteria has determined it is required. This may be based upon one or more factors: subject/category selections; age range values; number of records to be returned; request priority

[19] The FIS Roles assigned to a User will: specify the age ranges the user can enter for the selected subject/category; indicate if the user is able to select a non-default number of records to return; indicate if they are able to select match threshold and / or priority value; indicate if a specific subject/category combination will allow them to 'override' the authorisation requirement for a transcation.

Data		
	• System Username • Transaction Group ID • Transaction ID • Username • Requesting Agency	• Username • Transaction ID **Transaction** An audit record of the group transaction, and a transaction record for each selected data source, are created: • **Date/Time** • **Function** • **Requesting Agency** • **Username** • **System Name** • **Transaction Group ID** • **Transaction ID** • **Data Source** • Message Status • Message State • Message • **Transaction Status**

				Data		
						• **Probe MD5#** • Response MD5#'s • **Subject** • **Purpose** • **Category** • **Section** • **Minor Searched Indicator** • **Max Results Indicator** • **Match Threshold** • **Authorisation Override Indicator** • **Supervising Officer** • **Authorising Officer** • **Internal Reference Number**
2	The NEXIS Hub receipts, validates, and authenticates the request. Once authenticated, the request is routed to the selected Holding Agencies for processing.	The NEXIS Hub will capture audit metadata for the request.	• Data Sources • Facial Image • Gender • Purpose • Category • Subject • Act • Section • Supervising Officer • Authorising Officer	Validations occur • to verify the system user has the correct security privileges to submit this transaction. • To verify the	• Data Sources • Facial Image • Gender • Purpose • Category • Subject • Act • Section • Supervising Officer • Authorising Officer	**Transaction** The audit record of the group transaction, and a transaction record for each selected data source, are updated:

		Data		
	For each selected data source • Age Range • Number of records to be returned • Match threshold • Priority • System Username • Transaction Group ID • Transaction ID • Username • Requesting Agency	role assigned to the User allows them to submit the transaction type against the data source(es) • To verify data entered by the user is valid and allowed by their assigned role(s). Where it is determined Authorisation is required, a separate Authorisation process is initiated. The entire Transaction Group is delayed until Authorisation is provided.	*For each selected data source* • Age Range • Number of records to be returned • Match threshold • Priority • System Username • Transaction Group ID • Transaction ID • Username • Requesting Agency	• **Date/Time** • Function • Requesting Agency • Username • System Name • Transaction Group ID • Transaction ID • Data Source • Message Status • Message State • Message • **Transaction Status** • Probe MD5# • Response MD5#'s • Subject • Purpose • Category • Section • Minor Searched Indicator • Max Results Indicator • Match Threshold • Authorisation Override

			Data		
					Indicator - Supervising Officer - Authorising Officer - Internal Reference Number
For each Holding Agency selected					
3	The Holding Agency receipts, validates, and authenticates the request.	- Data Sources - Facial Image - Gender - Purpose - Category - Subject - Act - Section - Supervising Officer - Authorising Officer *For each selected data source* - Age Range - Number of records to be returned - Match threshold - Priority - System Username - Transaction Group	This is up to each Holding Agency, however typically they: - Ensuring the request is valid; and - Verifying information / attributes within the request.	This is up to each holding agency and how they have implemented their FIS services.	This is up to each holding agency and how they have implemented audit of their FIS services.

		Data	
		ID • Transaction ID • Username Requesting Agency	
4	The Holding Agency templates the probe image.	This is up to each holding agency and how they have implemented their FIS services.	This is up to each holding agency and how they have implemented audit of their FIS services.
5	The Probe Image template is compared against the entire set of image templates held at the Holding Agency. The highest match candidates above the match threshold (if any) are identified, the response encrypted, and returned to the NEXIS Hub.	This is up to each holding agency and how they have implemented their FIS services.	This is up to each holding agency and how they have implemented audit of their FIS services.
6	Once processed, the request is discarded.	This is up to each holding agency and how they have implemented their FIS services.	This is up to each holding agency and how they have implemented audit of their FIS services.

				Data		
Nexis Hub Processing						
7	The NEXIS Hub receipts, validates, and authenticates the response. Once authenticated, the response is routed to the Authenticated User. Each Holding Agency response is treated independently. As responses are received they are sent to the Authenticate User – the Hub does not wait for all response to be returned before processing and sending them to the Authenticated User.	The NEXIS Hub will capture audit metadata for the Response.	Information returned from each data source[20] • Transaction Group ID • Transaction ID • Priority • Message • Message State • MessageStatusCode For each returned record, the holding agency may provide: • Image • Image ID • Match Score • Image date of capture • Surname • Given Names • Gender • Customer ID • Document ID	Validations occur • to verify the system user has the correct security privileges to submit this transaction response, and • To verify the recipient of the transaction response;	• Transaction Group ID • Transaction ID • Priority • Message • Message State • MessageStatusCode For each returned record: • Image • Image ID • Match Score • Image date of capture • Surname • Given Names • Gender • Customer ID • Document ID • Document Type • Document Status • Data-source specific attributes	**Transaction** The transaction audit record for the specific data source is updated: • **Date/Time** • Function • Requesting Agency • Username • System Name • Transaction Group ID • Transaction ID • Data Source • **Message Status** • **Message State** • **Message** • **Transaction Status** • Probe MD5#

[20] While there are common elements of information that may returned from each holding agency, there are also specific data elements. Specific elements have not been captured here in detail. The attributes listed here are the generic ‘full’ set of elements that may be returned.

				Data		
			• Document Type • Document Status • Data-source specific attributes			• **Response MD5#'s** • Subject • Purpose • Category • Section • Minor Searched Indicator • Max Results Indicator • Match Threshold • Authorisation Override Indicator • Supervising Officer • Authorising Officer • Internal Reference Number
8	The Authenticated User is able to view that a response has been received from the Holding Agency.	The NEXIS Hub will capture portal metadata for the response	• Transaction Group ID • Transaction ID • Priority • Message • Message State • Message Status Code		• Transaction Group ID • Transaction ID • Priority • Message • Message State • Message Status Code	**User activity** An audit record is created to indicate the User has viewed the FIS transaction with the following information: • Date/Time

	Data		
	For each returned record: • Image • Image ID • Match Score • Image date of capture • Surname • Given Names • Gender • Customer ID • Document ID • Document Type • Document Status • Data-source specific attributes	For each returned record: • Image • Image ID • Match Score • Image date of capture • Surname • Given Names • Gender • Customer ID • Document ID • Document Type • Document Status • Data-source specific attributes	• Audit Type (e.g. User viewed the FIS Search response from <Data Source>) • Username • Transaction ID **Transaction** The transaction audit record for the specific data source is updated: • **Date/Time** • Function • Requesting Agency • Username • System Name • Transaction Group ID • Transaction ID • Data Source • Message Status • Message State

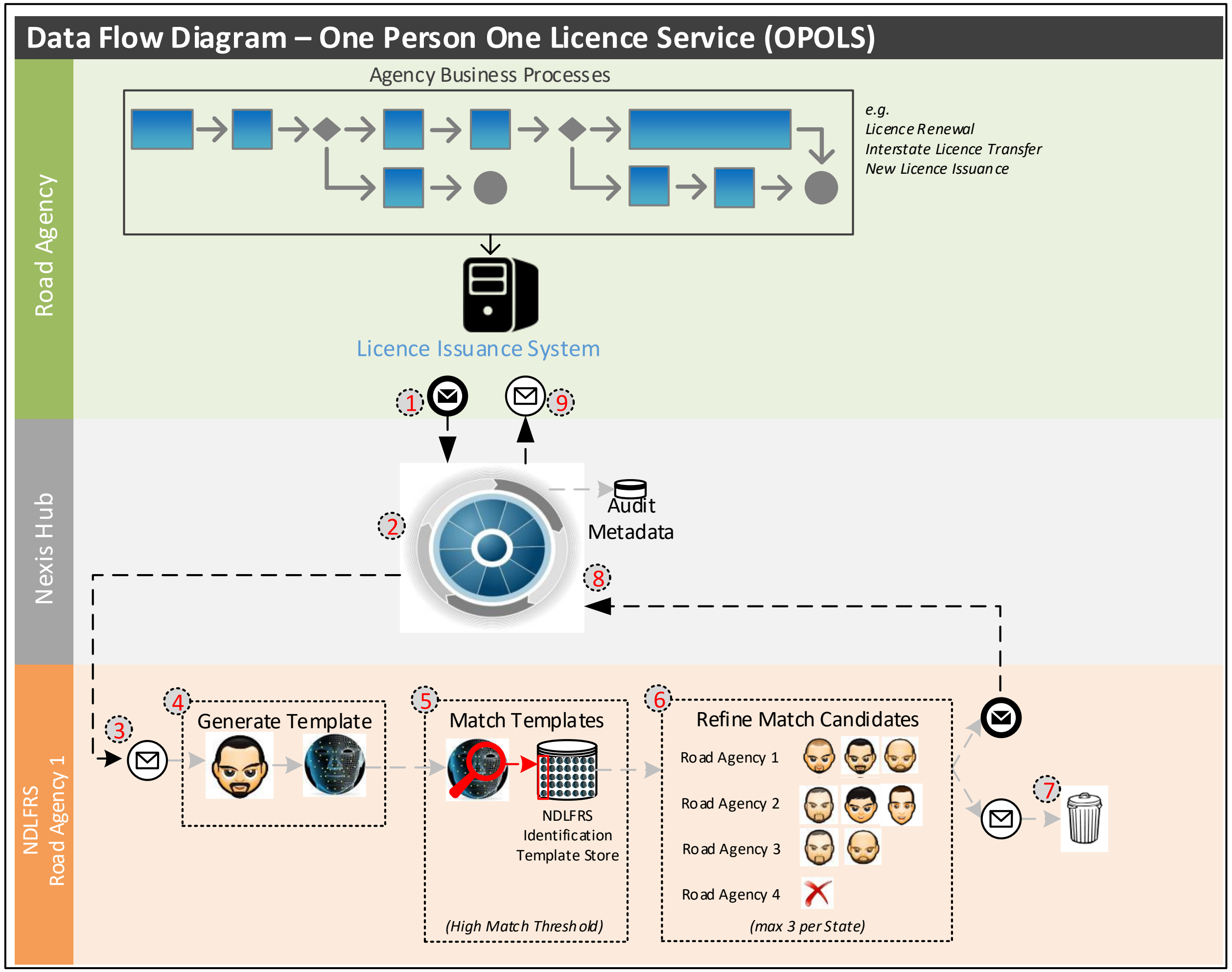
				Data		
						- Message - **Transaction Status** - Probe MD5# - Response MD5#'s - Subject - Purpose - Category - Section - Minor Searched Indicator - Max Results Indicator - Match Threshold - Authorisation Override Indicator - Supervising Officer - Authorising Officer - Internal Reference Number
9	The Authenticated User is able to view the gallery of match candidates. They are able to shortlist those match candidates they believe match the identity of the probe image (if any). After viewing the gallery and shortlisting any match candidates, the gallery result set is discarded and cannot be reviewed.	The User is only able to view the returned image from the data source. No other returned information about each record returned in the	- Transaction Group ID - Transaction ID - Priority - Message - Message State - Message Status	The Portal enforce the maximum limit of records that can be added to a shortlist as per what the Holding Agency has	- Transaction Group ID - Transaction ID - Priority - Message - Message State - Message Status	**Transaction** The transaction audit record for the specific data source is updated:

	Data				
	response is visible. The User is only able to shortlist the number of gallery records specified by the Holding Agency. The NEXIS Hub will capture metadata for User actions taken against the response Gallery.	Code For each returned record: • Image	specified.	Code For each shortlisted record, the following information may be added to the Shortlist: • Image • Image ID • Match Score • Image date of capture • Surname • Given Names • Gender • Customer ID • Document ID • Document Type • Document Status • Data-source specific attributes	• **Date/Time** • Function • Requesting Agency • Username • System Name • Transaction Group ID • Transaction ID • Data Source • **Message Status** • **Message State** • **Message** • **Transaction Status** • Probe MD5# • **Response MD5#'s** • Subject • Purpose • Category • Section • Minor Searched Indicator • Max Results Indicator • Match Threshold • Authorisation Override

			Data		
					Indicator - Supervising Officer - Authorising Officer - Internal Reference Number
10	The Authenticated User is able view, and add to, the shortlist result set for responses related to that FIS transaction.	The User is only able to view the Shortlist for a limited time (12 hours). After this the shortlist is discarded. The User is only able to add records to the shortlist which relate to that specific FIS transaction. They cannot add results from different FIS transactions to the same shortlist.	- Transaction Group ID - Transaction ID - Priority - Message - Message State - Message Status Code For each shortlisted record, the following information may be available: - Data Source - Image - Image ID - Match Score - Image date of capture - Surname - Given Names - Gender - Customer ID - Document ID		

Data
• Document Type • Document Status • Data-source specific attributes

10.3 OPOLS



Data

		Data				
#	Description	Notes	Inputs	Transformations / Processes	Outputs	Audit
1	A Road Agency Issuance System (or similar) submits an OPOLS query to NEXIS Hub via the Portal. The request is encrypted upon submission.		• Data Sources • Image • Gender • DoB • Priority • Match Threshold	Basic data entry validations are performed.	• Data Sources • Image • Gender • DoB • Priority • Match Threshold • System Username • Transaction Group ID • Transaction ID • Username • Requesting Agency	This is up to each Road Agency and how they have implemented audit of their OPOLS service.
2	The NEXIS Hub receipts, validates, and authenticates the request. Once authenticated, the request is routed to the NDLFRS for processing.	The NEXIS Hub will capture audit metadata for the request.	• Data Sources • Image • Gender • DoB • Priority • Match Threshold • System Username • Transaction Group ID • Transaction ID • Username • Requesting Agency • Match	Validations occur • to verify the system user has the correct security privileges to submit this transaction. • To verify the role assigned to the User allows them to submit the transaction type against the data source(es) • To verify data	• Data Sources • Image • Gender • DoB • Priority • Match Threshold • System Username • Transaction Group ID • Transaction ID • Username • Requesting Agency	**Transaction** An audit record of the group transaction is created: • **Date/Time** • **Function** • **Requesting Agency** • **Username** • **System Name** • **Transaction Group ID** • **Transaction ID** • **Data Sources**

			Data		
		Threshold	entered by the user is valid and allowed by their assigned role(s).	- Number of Records	- Message Status - Message State - Message - **Transaction Status** - **Probe MD5#** - Response MD5#'s
3	The NDLFRS receipts, validates, and authenticates the request.	- Data Sources - Image - Gender - DoB - Priority - Match Threshold - System Username - Transaction Group ID - Transaction ID - Username - Requesting Agency - Number of Records	Specific validation activities are still to be defined, however the general purpose of validations will be to: - Ensure the request is valid; and - Verifying information / attributes within the request. The age range values are determined based upon the DoB provided.	- Data Sources - Image - Gender - Age Range - Priority - Match Threshold - System Username - Transaction Group ID - Transaction ID - Username - Requesting Agency - Number of Records	**NDLFRS Transaction Audit** An NDLFRS audit record for the transaction is created:[21] - **Date/Time** - **Function** - **Requesting Agency** - **Username** - **System Name** - **Transaction Group ID** - **Transaction ID** - **Data Sources** - Message Status - Message State - Message - **Transaction**

[21] The final set of audit data to be captured as part of NDLFRS transactions is still to be finalised.

				Data		
						Status • **Probe MD5#** • Response MD5#'s
4	The NDLFRS generates an Identification Template for the Probe image.		• Image	The NDLFRS FR Engine produces a biometric template for the provided probe image.	• Probe Biometric template	**NDLFRS Transaction Audit** The NDLFRS audit record for the transaction is updated:[22]
5	The Probe Image template is compared against the entire set of templates held in the NDLFRS Identification Template Database. All match candidates above the defined match threshold (if any) are identified.		• Probe Biometric template • Match Threshold *From NDLFRS Template Data Store* • Set of existing NDLFRS Identification Biometric Templates & corresponding FR Entity ID's	A comparison of the Probe Biometric Template against all NDLFRS Identification Biometric Templates is executed.	• FR Entity ID's for records which matched the Probe Image at/above a the match threshold (high) • Match Score • Match Threshold	**NDLFRS Transaction Audit** The NDLFRS audit record for the transaction is updated:[23]
6	The resulting set of match candidates are then refined to identify only the top 2-3 match candidates and	Refinement criteria includes only those	• FR Entity ID's for records	Starting with highest matching FR Entity	• Match Threshold	**NDLFRS Transaction**

[22] The final set of audit data to be captured as part of NDLFRS transactions is still to be finalised.

[23] The final set of audit data to be captured as part of NDLFRS transactions is still to be finalised.

			Data		
associated DL record details for each Road Agency. Once refined, the response is encrypted and sent to the NEXIS Hub for routing to the Road Agency system.	which match the OPOLS request gender value, and have a DoB which falls 1-2 years each side of the request DoB.	which matched the Probe Image at/above a the match threshold (high) • Match Score • Match Threshold	ID's, a comparison of Gender and DoB is done until (up to) the top 2-3 matches for each Road Agency have been identified.	• System Username • Transaction ID • Username • Requesting Agency • Message • Message State • Message Status Code Data to be returned for each record may include:[24] • Customer ID • Data Source • DoB • Last Name • Given Name • Deceased Indicator • Gender • Address	**Audit** The NDLFRS audit record for the transaction is updated:[25]

[24] The data to be returned as part of an OPOLS transaction is still being finalised, and may also differ between RTAs as per what they have 1) agreed to replicate t the NDLFRS, and 2) what they have agreed to return in an OPOLS response.

[25] The final set of audit data to be captured as part of NDLFRS transactions is still to be finalised.

		Data	
		• Suburb • State • Postcode • Country • Document Type • Document ID • Document Issue Date • Document Expiry Date • Issue Location • Licence Class • Licence Class Expiry Date • Licence Endorsement • Licence Conditions • Card Number • Card Status • Card Issue Date • Card Expiry Date • Image Capture Date/Time • Image ID • Image • Match Score • Match Threshold • Match Indicator	
7	Once processed, the request is discarded.		**NDLFRS Transaction Audit**

				Data		
						The NDLFRS audit record for the transaction is updated:[26]
8	The NEXIS Hub receipts, validates, and authenticates the response. Once authenticated, the response is routed to the Road Agency.	The NEXIS Hub will capture audit metadata for the request.	- Match Threshold - System Username - Transaction ID - Username - Requesting Agency - Message - Message State - Message Status Code Data to be returned for each record may include: - Customer ID - Data Source - DoB - Last Name - Given Name	Validations occur - to verify the system user has the correct security privileges to submit this transaction response, and - To verify the recipient of the transaction response;	- Match Threshold - System Username - Transaction ID - Username - Requesting Agency - Message - Message State - Message Status Code Data to be returned for each record may include: - Customer ID - Data Source - DoB - Last Name - Given Name	**Transaction** An audit record of the group transaction is created: - **Date/Time** - Function - Requesting Agency - Username - System Name - Transaction Group ID - Transaction ID - Data Sources - Message Status - Message State - Message - **Transaction Status** - Probe MD5# - **Response MD5#'s**

[26] The final set of audit data to be captured as part of NDLFRS transactions is still to be finalised.

	Data	
	• Deceased Indicator • Gender • Address • Suburb • State • Postcode • Country • Document Type • Document ID • Document Issue Date • Document Expiry Date • Issue Location • Licence Class • Licence Class Expiry Date • Licence Endorsement • Licence Conditions • Card Number • Card Status • Card Issue Date • Card Expiry Date • Image Capture Date/Time • Image ID • Image • Match Score • Match	• Deceased Indicator • Gender • Address • Suburb • State • Postcode • Country • Document Type • Document ID • Document Issue Date • Document Expiry Date • Issue Location • Licence Class • Licence Class Expiry Date • Licence Endorsement • Licence Conditions • Card Number • Card Status • Card Issue Date • Card Expiry Date • Image Capture Date/Time • Image ID • Image • Match Score • Match

		Data		
		Threshold • Match Indicator	Threshold • Match Indicator	
9	The Road Agency Issuance System receives and processes the response.	• Match Threshold • System Username • Transaction ID • Username • Requesting Agency • Message • Message State • Message Status Code Data to be returned for each record may include: • Customer ID • Data Source • DoB • Last Name • Given Name • Deceased Indicator • Gender • Address • Suburb • State • Postcode • Country • Document Type • Document ID • Document Issue		This is up to each Road Agency and how they have implemented audit of their OPOLS service.

Data
Date • Document Expiry Date • Issue Location • Licence Class • Licence Class Expiry Date • Licence Endorsement • Licence Conditions • Card Number • Card Status • Card Issue Date • Card Expiry Date • Image Capture Date/Time • Image ID • Image • Match Score • Match Threshold Match Indicator

11. Appendix E – Possible risks against the APPs

This table considers the application of the APPs to the NDLFRS. In accordance with the scope for this PIA risks are assessed primarily from the perspective of AGD's management of the NDLFRS. Where risks are affected by the NDLFRS data sources or use cases this is also noted. The analysis here is high-level and intended to flag issues. The issues identified are discussed, with other privacy risks, in Section 6 above.

APP summary	**Design –** Architecture, data replication and security protocols	**Operation –** Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)	**Governance** Arrangements, participation of data owners, and consumers
Demonstrated APP compliance – practices, procedures, systems (APP 1.2)	N/A to design	If AGD does not have, or does not implement a privacy management plan and/or plan to monitor its and other users compliance with NDLFRS use obligations there could be more likelihood it would be in breach of the Privacy Act and/or of breaches or policy changes negatively affecting individuals. Low risk – *AGD has committed to PbD, and to 'maintaining robust privacy safeguards in the design, implementation and ongoing*	If the governance arrangements, including the IGA, do not include requirement for RTAs to demonstrate privacy compliance in the context of the NDLFRS, AGD might not be able to provide assurance that personal information is appropriately protected. *Medium risk – governance material including the IGA incorporate various measures in this regard. IIS has identified some additional measures* (see Section

APP summary	Design – Architecture, data replication and security protocols	Operation – Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)	Governance Arrangements, participation of data owners, and consumers
		management of the NDLFRS and its Services.'[27] AGD advises it would have a privacy policy, compliance policy and a register of key decisions made about technical design aspects. It is also working with OAIC on an annual audit program.	6.4)
Openness – privacy policies (APP 1.3 and 1.4)	N/A to design	If AGD does not provide information about its role in the NDLFRS it might not be complying with the Privacy Act. While the privacy policy might not be the main way that individuals become aware of AGD's role, it would be one element promoting transparency. *AGD's privacy policy provides some detail about the sort of information it holds but does not currently reference the NFBMC or the DVS.*	Various transparency issues identified – see specific points on governance in Section 6.4.

[27] AGD response to Recommendation 1, NFBMC preliminary PIA

APP summary	Design – Architecture, data replication and security protocols	Operation – Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)	Governance Arrangements, participation of data owners, and consumers
		While a lower risk area, a more detailed policy appears appropriate.	
Anonymity and pseudonymity (APP 2)	APP 2 provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with agencies or organisation subject to the Privacy Act. APP 2 does not apply where agencies or organisations are required or authorised by law to deal with identified individuals or where it would be impractical for the individual to remain anonymous or adopt a pseudonym. One or other of these exceptions is likely to apply in the context of the NFBMC. The IGA provides that that 'While the sharing of identity information through the Identity Matching Services limits the right to anonymity, this limitation is reasonable, necessary and proportionate'.		
Collection – necessary, lawful and fair and direct, consent needed to collect biometric information unless exceptions apply (APP 3)	If the NDLFRS design results in collection of more information than is needed and in particular, more sensitive information, this could affect community acceptance and potential risks for individuals, as well as compliance risks. *Low risk– Hub design aims to retain minimum information and this would be defined in the proposed legislation to support the NFBMC. NDLFRS would hold personal information, including some sensitive information, in jurisdiction partitions (AGD does not*	Risk of non-compliance when collecting sensitive information, including biometric information without consent, unless the collection is required or authorised by law, or the information is collected by an enforcement agency where the collection is reasonably necessary, or directly related to, its functions. *IIS understands AGD's collection of sensitive information would be authorised by the proposed Commonwealth legislation for the NDLFRS and/or it would be an*	If governance arrangements do not underpin policy intent to limit information held, actual nature of information held would be less clear, and potential for information to be used for unexpected or new uses. *There is a technical ability for jurisdictions to include information used on documents other than driver licences in the NDLFRS, where disclosure of this information to the Commonwealth is authorised in state legislation, and where the Commonwealth's collection, use and disclosure of this information is authorised*

APP summary	**Design –** Architecture, data replication and security protocols	**Operation –** Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)	**Governance** Arrangements, participation of data owners, and consumers
	have direct access). *There would be an audit trail for NDLFRS information accessed through the Face Matching Services. The information retained is limited and needed to offset security risks. It would include the entity that accessed the image but would be practically very difficult to use this to track an individual's activities.*	*enforcement agency under the Privacy Act. IIS notes that while not directly considered by this PIA, consent processes will be relevant in some circumstances to access to NDLFRS information, see Section 6.3.2.2* If operational decisions result in the collection of more information than is needed and in particular, more sensitive information, this could affect community acceptance and potential risks for individuals, as well as compliance risks. *AGD is actively seeking to limit information held in the context of the NDLFRS to that necessary for the proposed purposes, including by defining 'identification information' in the proposed new Commonwealth legislation for the NDLFRS.* *The IGA and other agreements would set limits on what information can be*	*in Commonwealth legislation (including the proposed new legislation for the NDLFRS). It would be up to states and territories to decide if requesting entities can access the information. This would be a matter for states and territories PIAs.*

APP summary	Design – Architecture, data replication and security protocols	Operation – Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)	Governance Arrangements, participation of data owners, and consumers
		used for what purposes.	
Dealing with unsolicited personal information (APP 4)	Not relevant for NDLFRS	Not relevant for NDLFRS	Not relevant for NDLFRS
Notice/Transparency (APP 5)	N/A to design	If AGD treats NDLFRS information as personal information, it would have obligations to take reasonable to steps to give individuals notice of matters specified in APP 5.2. If steps are not taken, individuals would not be fully informed about possible face matching uses, which might affect the choices they make or consent processes. *The IGA does include obligations on Participating Agencies to provide some information about disclosures to the Commonwealth. More detailed information is likely to be needed. AGD advises this can be covered in the NDLFRS Hosting Agreement.*	If there are variations in transparency approaches in jurisdictions, including because no privacy law applies, individuals might act on incomplete information or might have difficulty in understanding and sorting out sources of problems. *As noted, the IGA includes some but not comprehensive privacy notice requirements*.
Limits on use and disclosure (APP 6)	N/A to design	If state and territory agencies are not authorised to collect, use or disclose	Governance arrangements would be part of the framework to ensure all

APP summary	**Design – Architecture, data replication and security protocols**	**Operation – Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)**	**Governance** **Arrangements, participation of data owners, and consumers**
		images and/or biographic and related drivers licence information for specified purposes, risk of privacy breach, and impact on trust in processes. *AGD and stakeholders have identified this as an issue. AGD considers the proposed Commonwealth legislation, the IGA and the legally binding Participation Agreement as providing the authorisation framework. Also building on compliance processes and transparency reporting.* *AGD is also proposing that some use of the Face Matching Services involving NDLFRS data, for example, private sector use of the FVS, would be authorised on the basis that individuals have given consent.* *The approach taken to consent would affect the privacy impacts (see Section 6.3.2.2).*	Participating Agencies are authorised to collect, use and disclose NDLFRS information and that they then only collecting, using and disclosing information in ways permitted. *The legal authorities for jurisdictions will be canvassed in separate states and territories PIAs.* *In addition the governance arrangements include various transparency and assurance processes. There are some possible gaps in these arrangements (see Section 6.4).*

APP summary	Design – Architecture, data replication and security protocols	Operation – Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)	Governance Arrangements, participation of data owners, and consumers
Direct marketing (APP 7)	Not relevant for NDLFRS	Not relevant for NDLFRS	Not relevant for NDLFRS
Transborder data flows (APP 8)	The Hub and NDLFRS will be hosted in Australia. *No issues identified at this point.*	*No issues from AGD perspective.*	*Jurisdictions would have transborder obligations. IIS presumes these issues would be tested in the jurisdiction PIAs.*
Unique identifiers (APP 9)	The NDLFRS (and AGD) would be collecting, using and disclosing identification information including driver licence (unique identifier) details from the jurisdictions' NDLFRS partitions. *AGD activities involving driver licence details would be consistent with APP 9 to the extent that they are authorised by law (covered in the proposed Commonwealth legislation), or other exceptions apply.* *No privacy risks identified from a design perspective.* *No issues from AGD perspective.*		*Possible issues for the states and territories that IIS considers would need to be tested in their PIAs.*
Quality/Accuracy (APP 10)	If the Face Matching Services produces false negative matches, or there are data design or syncing processes that introduce or magnify accuracy issues in jurisdictions' data, there is potential for significant impact on individuals.	If AGD does not address data accuracy risks in setting up and managing NDLFRS again, potential impact on individuals. Risk that NDLFRS operational arrangements do not give sufficient emphasis to identifying and dealing	Risk that NDLFRS governance arrangements do not give sufficient emphasis to identifying and dealing with quality or accuracy issues for the NDLFRS. *Steps being taken but might not be sufficient emphasis in ensuring that risks*

APP summary	Design – Architecture, data replication and security protocols	Operation – Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)	Governance Arrangements, participation of data owners, and consumers
	AGD is taking steps to minimise impact of accuracy issues arising from the NDLFRS design and processes including drawing on experience with DVS, testing face-matching systems, and working with jurisdictions on data accuracy issues. It would be important for AGD and other participants to be aware of and manage the risks here. (See Section 6.3.3).	with quality or accuracy issues. *It would be important for AGD and other participants to be aware of manage the risks here. (See Section 6.3.3).*	*are not transferred to individuals. (See discussion at Section 6.4).*
Storage and security (APP 11.1)	If system design or implementation inadequate, potential for data breaches. *Security a strong focus at all levels – no design issues identified.*	If security measures or assurance processes are insufficient, potential for data breaches. *AGD is adopting a multi-layered approach involving systems, staff and assurance within the NDLFRS and in Participating Agencies. In discussions with privacy regulators, additional steps to actively monitor the audit logs were recommended. Monitoring practices should be informed by information about potential nefarious activities. (See Section 6.4.4)*	If proposed governance arrangements, which call for strict security and assurance processes, are not implemented or implemented well, there are potential for risks to individuals and to trust in the system. *Range of positive measures proposed. In discussions with privacy regulators, additional steps to actively monitor the audit logs were recommended. (See Section 6.4.4)*

APP summary	Design – Architecture, data replication and security protocols	Operation – Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)	Governance Arrangements, participation of data owners, and consumers
Retention (APP 11.2)	If system design or implementation of the NDLFRS is inconsistent with data retention policies, there is the potential for information to be retained unnecessarily, adding to security and data breach risks. *Policy decisions still being finalised on nature of, and timeframes for, retention of data for audit purposes. No design issues identified at this point.*	If formal data retention policies, which take into account privacy risks, are not in place, there is the potential for audit data to be retained when it is no longer needed, increasing security and other risks. *Formal policies not yet in place – some approaches being developed, for example, with respect to replacement of more up-to-date templates in the image store. (See Section 6.3.4).*	*Possible issues for the jurisdictions that IIS considers would need to be tested in jurisdiction PIAs.*
Access and correction (APPs 12, APP 13)	N/A to design	If AGD and states and territories do not work out roles and responsibilities or do not provide adequate resources individuals might have difficulty making requests or resolving issues. *AGD anticipates that it would be responsible for handling requests. It is not yet clear on how processes would work but anticipates coordination with the states and territories. It has allocated some resources for*	*Possible issues for the jurisdictions that IIS considers would need to be tested in jurisdiction PIAs.*

APP summary	Design – Architecture, data replication and security protocols	Operation – Technical implementation of FM requests, AGD role and responsibilities, RTAs responsibilities and obligations (accuracy, notice, inquiries)	Governance Arrangements, participation of data owners, and consumers
		assistance to individuals making inquiries. (See Section 6.3.5)	

INFORMATION
INTEGRITY
SOLUTIONS

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898