National Facial Biometric Matching Capability

Privacy Impact Assessment:

AFP Access to DIBP FVS (Match & Search Functions) for Citizenship & Visa Images

Version 1.0.1

Stephen Wilson
Lockstep Consulting
August 2016

Consulting report

NFBMC FVS Match & Search Functions PIA

Version 1.01

For National Facial Biometric Matching Capability

[Lockstep NFBMC PIA Report 4 - Match and Search Functions DIBP-AFP (1.01)]

Stephen Wilson

ABN 17 582 844 015

PUBLIC

Lockstep Consulting (est. 2004) provides independent research, analysis and advice on digital identity, privacy, cyber security policy and strategy, and e-business risk management.

http://lockstep.com.au

Table of Contents

Executive Summary

Lockstep Consulting was engaged by the Attorney-General's Department to undertake a set of Privacy Impact Assessments on the different functions of the Face Verification Service (FVS) within the National Facial Biometric Matching Capability. Lockstep was asked to evaluate any privacy impacts that may be associated with the proposed use of the different FVS functions in which the Department of Immigration and Border Protection (DIBP) will provide facial biometric data and/or match results in response to requests from the Department of Foreign Affairs and Trade (DFAT) or the Australian Federal Police (AFP).

Four reports were commissioned at this stage:

1. FVS *Retrieve* function between DIBP and DFAT;
2. FVS *Retrieve* function between DIBP and the AFP;
3. FVS *Match* and *Search* functions between DIBP and DFAT;
4. FVS *Match* and *Search* functions between DIBP and AFP (this report).

The NFBMC's general objective is to utilise the considerable facial biometric holdings across government to prevent fraud, support law enforcement, promote community safety and streamline service delivery, such as assisting DFAT staff to confirm the identity of naturalised citizens applying for a passport. The NFBMC is a key initiative under the *National Identity Security Strategy* and the *National Biometric Interoperability Framework*. The NFBMC program is designed to enhance the ability of authorised government agencies to share and match facial images against the records of other participating agencies in a more secure, automated and accountable way than is the case with current manual processes. In the longer term, one-to-many searching for facial *identification* is planned; however the initial rollout is deliberately restricted to the functions of one-to-one image retrieval and matching that entail lesser privacy impacts.

The FVS is architecturally similar to the Document Verification Service (DVS) in that it is supported by a central hub service providing a uniform set of interfaces whereby agencies that hold identity data can provide extracts or derivatives of that data on request to other authorised agencies. The FVS hub will retain no Personal Information about members of the public in these transactions, but it will log the fact of each inquiry together with pseudonymised details of which authorised agency users were involved. The FVS will enforce strict access arrangements that must be struck between all participating agencies. The current FVS functionality will not entail any changes to the legislative basis for sharing biometric data amongst DIBP and the AFP.

Overall we find that changing from manual exchange of biometric data between DIBP and the AFP to using the FVS to share that data via the *Match* and *Search* functions will be privacy positive, for it will reduce the volume of Personal Information being disclosed and aggregated locally. Further, the FVS will serve to restrict biometric data flows to authorised parties at the AFP through a rigorous Access Policy and strong access

controls, and the FVS will create clear audit trails of who at the AFP is responsible for every individual biometric data request.

Nevertheless, privacy risks and public concerns can be expected to mount with the increasing sophistication of FVS *Match* and *Search*. These types of operations are not readily carried out manually, so their emergence in the NFBMC might presage more automated use of biometrics in future. Lockstep therefore recommends the following actions to mitigate privacy risks arising from FVS:

Recommendations

1. AGD should consider creating a privacy statement specific to the FVS hub, to address generally recognised privacy concerns around biometrics (such as the limits to sharing of biometrics), and to explain to the public the major data protection properties of the NFBMC. Such a privacy statement could cover the NFBMC design philosophy, key procedural and technological data protection measures, and the high level rules, like DIBP and AFP being required to enter into a bilateral data sharing agreement, and publish this PIA.
2. The FVS portal, at the time that a *Match* or *Search* is requested, should display a reminder to users of their obligations as officers of AFP to treat all Personal Information in accordance with the Privacy Act and other relevant terms of their employment conditions.
3. Ensure that the AFP understands the limited event logging of the hub, and the need to cater for its own logging and auditing requirements. In particular, ensure that AFP system designers understand that biometric algorithm and matching parameters are not retained by the FVS or the hub and may not be made available by the FVS or the hub if ever needed.
4. AGD should consider adding advice to the IDSA guidance that requesting agencies (AFP in this case) locally record details from time to time of the biometric algorithms used by the holding agency (DIBP here), in case future investigations of, for example, false matches, need to reference the algorithms and parameters applied in each usage of the FVS.
5. The AFP should retain its own records of all biometric matching parameters and other configuration information (algorithms, biometric product version numbers etc.) used by DIBP to produce each *Match* or *Search* result. Algorithm updates, especially changes to threshold parameters used for matching or searching, will change the performance of the processes from time-to-time, and these changes should be tracked by the AFP, so that in the event that a dispute arises, the precise conditions of past matches are not lost.

Glossary

Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
Sensitive Information	(a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) criminal record; that is also Personal Information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

Acronyms

AFP	Australian Federal Police
AGD	Attorney-General's Department
API	Application Programming Interface
APO	Australian Passport Office
APP	Australian Privacy Principle
DFAT	Department of Foreign Affairs and Trade
DIBP	Department of Immigration and Border Protection
DVS	Document Verification Service
EOI	Evidence of Identity
FIS	Face Identification Service
FVS	Face Verification Service
ICSE	Integrated Client Services Environment system
IDSA	Interagency Data Sharing Agreement
IDSS	Identity Data Sharing Service

IGA	Intergovernmental Agreement [on Identity Matching Services]
IOH	Interoperability Hub
IP	Internet Protocol
IRAP	Infosec Registered Assessors Program
IRU	Identity Resolution Unit
ISM	Information Security Manual
LEA	Law Enforcement Agency
MD5	Message Digest number Five (a hash algorithm)
NFBMC	National Facial Biometric Matching Capability
NISS	National Identity Security Strategy
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment
POI	Proof of Identity
PSPF	Protective Security Policy Framework
SDLC	Software Development Lifecycle
SRMP	Security Risk Management Plan
TRA	Threat & Risk Assessment

The Australian Privacy Principles

APP 1: Open and transparent management of Personal Information
APP 2: Anonymity and pseudonymity
APP 3: Collection of solicited Personal Information
APP 4: Dealing with unsolicited Personal Information
APP 5: Notification of the collection of Personal Information
APP 6: Use or disclosure of Personal Information
APP 7: Direct marketing
APP 8: Cross-border disclosure of Personal Information
APP 9: Adoption, use or disclosure of government related identifiers
APP 10: Quality of Personal Information
APP 11: Security of Personal Information
APP 12: Access to Personal Information
APP 13: Correction of Personal Information.

Introduction

Lockstep Consulting was engaged by the Attorney-General's Department to conduct a set of Privacy Impact Assessments on the design of the Face Verification Service (FVS) component of the National Facial Biometric Matching Capability. The program plans to roll out successively more complex FVS functionality through 2016, starting with image retrieval and progressing to image matching and image search, and is seeking to understand the privacy implications in an incremental manner.

Scope

This PIA Report 4 examines the information flows and privacy impacts of the AFP making *Match* and *Search* inquiries through the FVS hub against DIBP's holdings of facial images in citizenship and immigration-related databases.

The focus of this and the other three related FVS PIAs is privacy of members of the public who are subject to biometric matching transactions. Unless noted otherwise, "Personal Information" in this report means Personal Information of a member of the public, and not that of agency staff members using the FVS.

Approach and Methodology

This assessment involved a desktop review of NFBMC project documentation, requirements analysis, architectural details and the initial PIA [6], followed by group interviews with AGD, DIBP and AFP personnel. Additional desk top review of cited materials, and several rounds of questions-and-answers followed.

The FVS project is still in development, and therefore a number of functional specifications were finalised as this assessment proceeded, and were made available to us as they became available (eg [12][13][14][15]).

The PIA was conducted by Stephen Wilson, Principal Consultant, Lockstep Consulting.

Reference frame

The PIA was conducted under the Australian Privacy Principles (APPs) set out in the *Privacy Act 1988*.

Important disclaimer

The consulting advice in this document does not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Lockstep Consulting is not a law firm. No legal professional privilege applies to this report.

Description of the project

Overview

The National Facial Biometric Matching Capability (NFBMC) is intended to "help government agencies combat identity crime, organised crime and terrorism. It aims to enable law enforcement and selected government agencies to share and match photographs on identity documents such as passports to strengthen identity-checking processes, while maintaining strong privacy safeguards"[30]. Name-based identity checking has recently been named in the Martin Place Siege Inquiry as a major problem, and biometrics have the potential to improve policing and crime prevention [29].

AGD plans a staged rollout of NFBMC functionality through 2016-17, and an incremental series of PIAs. The project is currently assessing the privacy impacts of the Face Verification Service and its three principal functions: *Retrieve*, *Match* and *Search*. The initial PIA has recently been completed and published [6] and was followed by focused PIAs of the FVS *Retrieve* function for DFAT [16] and for the AFP [17]. In summary, the Match and Search functions are distinct from the Retrieve function in that they involve facial biometric matching whereas Retrieve involves the return of a facial image in response to a text-based search. Match involves a check against a particular record identified by a unique identifier such as a document number. Search involves a check of one or multiple records with matching biographic details, in order to return a single matching record. Details of the Match and Search functions will be described later in this report.

The NFBMC will provide services to approved participating agencies, which will be required to comply with rigorous business rules and technical standards. Access to the NFBMC online services will be restricted to identified individuals within those agencies. Initially, most access will be manual, through a web portal; little automated (programmed or scripted) access is envisaged at this stage, although there will be a transition to automated access over time. We discuss this in more detail below.

Initial FVS deployment is restricted to three agencies: DFAT and the AFP as major users of facial biometric data (in passport and other Australian travel document processing and in investigations respectively), and DIBP as a major source of facial image data. This PIA report is one of four in an initial set, and covers the use by the AFP of the two related FVS functions *Match* and *Search* to attempt to match a given image in DIBP's citizenship and visa related collections. The other three reports in the initial PIA set cover FVS *Retrieve* for DIBP to DFAT (Report 1), FVS *Retrieve* for DIBP to AFP (Report 2), and FVS *Match* and *Search* for DIBP to DFAT (Report 3).

Privacy Context

Data sharing arrangements in relation to citizenship and immigration related data are already in place between DIBP and the AFP, which uses facial images in the performance of its functions, particularly criminal and national security investigations.

Most credential issuing, law enforcement and national security agencies collect, use and seek to match facial biometric data as part of their operations. The sharing of facial biometric and associated identifying information between Commonwealth, state and territory agencies via the FVS will be governed by a proposed Intergovernmental Agreement on Identity Matching Services (IGA). Current manual methods for requesting raw biometric data and matching services are covered by laws and regulations, but the methods are cumbersome and are difficult to oversee or audit for consistency. The timely discovery of important policing information in existing facial image stores is thus sometimes impeded. There is evidence that better sharing of facial biometrics will help law enforcement and national security [29].

Pursuant to the IGA, participating agencies will need to comply with the FVS Access Policy [1] and enter into interagency data sharing agreements that meet requirements set out in a template developed by AGD [2].

The FVS will automate the retrieval, matching and searching of face images on a one-to-one basis, leading to more efficient identity verification and better "time to insight" in law enforcement activities. The FVS will not expand agencies' powers to deal with biometrics or other Personal Information, and at this stage will not affect their biometric collection practices or holdings. DIBP and AFP will rely on existing legal authority to collect, use and share facial images and related Personal Information via the FVS, as they do for current manual data sharing processes.

NFBMC philosophy

The biometric matching capability is being architected according to a number of expressly privacy enhancing functions, as follows.

- Use of the new hub will only come after confirming the legal permissibility and justification for use of biometrics by the participating agencies
- Formal bilateral data sharing agreements (IDSAs) are required between each pair of holding and inquiring agencies. AGD has developed a template agreement [2].
- Further, a PIA and Security Risk Management Plan must be completed by each participating agency and submitted to AGD before access will be allowed.

— No Personal Information about members of the public will be retained at the hub. Minimal audit logs will be retained sufficient for oversight purposes to be able to unambiguously show which authorised agency users performed which actions using the FVS (see also discussion of the image hash values below). Agencies will remain responsible for their own detailed event logging, and for determining what Personal Information if any they will log in their systems, as they must now.

— NFBMC functionality will be rolled out in stages and be restricted to a few agencies, starting with the use of the FVS among the AFP and DIBP as covered by this PIA and the related assessments [12][17].

— Agencies retain policy responsibility for biometric template matching. The technical details of biometric processing and matching (which are evolving rapidly in the industry) will properly remain the business of agencies. The detailed needs of requestors and the ability of holding agencies to help with them, are matters to be negotiated and supported by agencies, without involving AGD nor the NFBMC.

The NFBMC will not be used for minor offences such as littering or parking infringements.

The hub concept

To enhance privacy, the NFBMC follows a 'hub-and-spoke' architecture pattern. This approach avoids a large central database, and has been successfully used by the national Document Verification Service (DVS), which is also operated by AGD. The NFBMC's central Interoperability Hub will not store any biometric or biographic information, nor will it perform any matching. All matching occurs within the participating agencies that operate their own facial matching technology. The Hub will simply broker secure, automated and auditable sharing of facial images and related data between the participating agencies. The Hub will operate within existing privacy legislation, and agencies using the system will need to have the legislative authority to collect, use, store and disclose facial images, just as they do currently.

NFBMC should lead to consistent, auditable access to biometric matching, and (eventually) searching services, for an agency with a need to check a facial image on hand, against faces held by another agency. Crucially, the NFBMC hub will not perform any matching itself; all biometrics operations, processing and accountabilities will remain with responsible agencies. This demarcation strengthens limitations on collection and use of Personal Information.

The NFBMC will save agencies from needing to create and maintain redundant agency-to-agency biometric matching interfaces. Importantly however, it does not remove the need for inter-agency agreements; these will be one of the most important privacy protection planks of the new system.

Note that every request must be directed to a specific holding agency, with a data sharing agreement already in place with the requesting agency and a copy provided to AGD. Any request to the hub that tries to access data at an agency where there is no data sharing agreement in place with the requestor, or where the other mandatory security and privacy arrangements are not in place (per [1]) will be automatically rejected by the hub.

No Personal Information about members of the public will be retained at the hub (see also APPs assessment below). Minimal details about an individual who is the subject of a *Match* or *Search* request will be cached (held in temporary memory) during a session in which incoming requests are serviced by a holding agency; at the end of the session, the cache is purged and a minimal amount of data is logged for the purposes of monitoring and oversight. Personal Information is only used at the hub itself in order to transform data between agency formats. The NFBMC architecture essentially passes through data from requesting agency to the holding agency and back again. See APP 6 assessment below for further details. Some Personal Information about authorised agency users is logged at the hub for audit purposes. This information is in the form of pseudonymous usernames which are not identifiable to AGD, but are identifiable when combined with other information held by the requesting agency. It should be generally understood by users of biometrics technologies in government that their usage will be monitored, as part of normal staff accountability processes.

The logging of photo hash values

The hub will retain in its audit logs a hash value of every photograph that is sent with each *Match* and *Search* request. The purpose of this collection and retention is to allow investigation when necessary of the precise data that flowed for any given transaction with the hub. The technical nature of a hash value (calculated by an algorithm such as MD5 in the case of the NFBMC currently) is that the hashed data is unique to the original photo concerned but cannot be used to reconstruct that photo. The hash is sometimes referred to as a "thumbprint", for it is unique to the photo. In the event of any change to or substitution of the photo, the re-calculated hash value will always be different. No two photos, even of the same person taken at the same time under identical circumstances will ever generate the same hash value, thanks to the sensitivity of the algorithm. The purpose of the hash is to prove that a given photo was involved in a given NFBMC transaction. Without the given original photo, the hash cannot be used to reconstruct any Personal Information.

Security and access controls

Multiple layers of logical access control are included in the design to tightly lock down access to authorised personnel [1]. Authentication mechanisms include username and password, an X.509 digital certificate issued by AGD only to named authorised agency users, and IP address white-listing (whereby the precise office location of each authorised user's computer is known to the hub access control system; attempts to gain entry, even by legitimate users from unexpected locations, will be blocked).

Training and management of FVS users

Access to the FVS will only be provided to nominated users from requesting agencies, restricted to employees of those agencies who have a reasonable need to use the FVS to fulfil the functions of their employment. Agencies will manage the number of nominated users and maintain user records which will be subject to audits.

Nominated users will be required to undertake training on privacy, security and interpreting the results of the FVS. Access to FVS *Match* and *Search* functions will only be provided to AFP staff who have been trained in facial recognition and are able to accurately interpret the results.

Hub connection options

Agencies participating in the FVS may connect to the hub via one of two means: a web-based portal for human users, and automated system-to-system connections. The portal enables nominated users to submit queries individually, entering data manually. While queries are submitted manually, the response from the holding agency will be automated and returned via the portal.

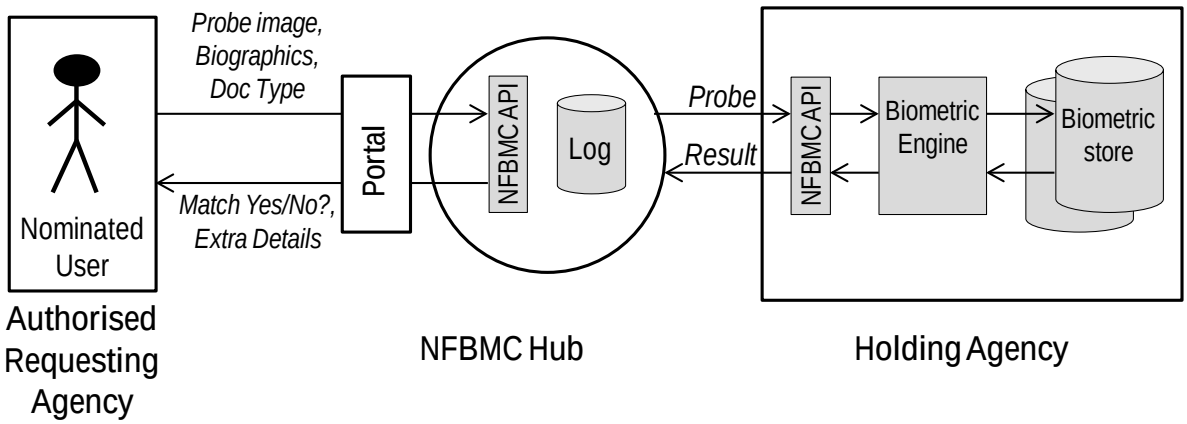
There will be a number of APIs for agencies to establish system-to-system connections with the hub. These will enable agencies such as the AFP to automate the submission of queries via the hub, either individually or in batches. This will enable agencies to incorporate an automated FVS query as part of a standard business process that requires verification of a person's identity, for example investigating crimes. System-to-system connections will operate within appropriate access permissions and privacy controls, with auditability similar to human users. AGD envisages that the AFP will use the portal in the first instance, before adopting a system-to-system connection over time. Further privacy impact assessment is advisable as automated Match and Search becomes available via the APIs.

The FVS *Match* and *Search* functions

The following figure depicts the FVS hub-and-spoke architecture, through which a nominated user at a requesting agency (AFP in this instance) may direct a *Match* or *Search* request to a holding agency (DIBP for now), and have responses returned, via the interoperability hub portal.

In future, these APIs will be exposed for use in automated system-to-system connections between the requesting agency and the hub. Initially however, access to DIBP data via the FVS will only be implemented in a manual mode using the hub portal.

Face Verification Service MATCH / SEARCH



Two of the service requests designed into the hub are relevant to this PIA: the closely related *VerifyMatchBiometricRequest* (see *Interface Requirements* in [12] & [14]) and *SearchBiometricRequest* (see *Interface Requirements* in [13] & [15]).

The *VerifyMatchBiometricRequest* enables AFP to search for a facial image and biographic information relating to a particular document in DIBP's citizenship and visa data sources, using that document ID, together with biographic details.

This function takes the following inputs:

- *Probe Image (Mandatory)*
- *Document Type (Mandatory, indicating either citizenship or visa store)*
- *Visa Type (Mandatory if visa holding is selected)*
- *Document ID (Mandatory)*
- *Family Name (Mandatory)*
- *Given Name (Optional)*
- *Date of Birth (Mandatory)*.

VerifyMatchBiometricRequest returns the following data for just one match if a match is found (or no data if no match is found):

- *Match flag*
- *Match value*
- *A facial image (if one is available)*
- *Biographical details including name, date of birth, gender, place of birth, country of birth, deceased indicator, alias indicator and for each alias, the name, date of birth and gender.*
- *If citizenship is selected, the citizenship status, document status (for Match function) are also returned*

- *If visa is selected, the country of citizenship, lawful status, visa grant number, visa class, visa subclass, visa status, visa grant date, and visa effective date are also returned.*

SearchBiometricRequest enables AFP to search for a facial image and biographic information in DIBP's citizenship and visa data sources, using a facial image and certain biographic details.

This function takes the following inputs:

- *Probe Image (Mandatory)*
- *Document Type (Mandatory, indicating either citizenship or visa store)*
- *Visa Type (Optional if visa holding is selected)*
- *Family Name (Mandatory)*
- *Given Name (Optional)*
- *Date of Birth (Mandatory)*.

SearchBiometricRequest returns the following data for just one match if a match is found (or no data if either no match, or multiple matches above the match threshold, are found):

- *Match flag*
- *Match value*
- *A facial image (if one is available)*
- *Biographical details including name, date of birth, gender, place of birth, country of birth, deceased indicator, alias indicator and for each alias, the name, date of birth and gender.*
- *If citizenship is selected, the citizenship status, document status (for Match function) are also returned.*
- *If visa is selected, the country of citizenship, lawful status, visa grant number, visa class, visa subclass, visa status, visa grant date, and visa effective date are also returned.*

Information flow mapping

Existing flows

Currently the major flows of Personal Information and face biometric-related data from DIBP to AFP are via separate inquiries initiated by police officers. There is a convention that all requests lodged with DIBP by an AFP officer need to cite the reason and legal justification for obtaining the data concerned. Requests are usually lodged by email to a shared group email box at DIBP. This practice will produce something of a uniform audit trail at such email boxes, however there is no guarantee that we can see that requests are not lodged in other channels. Further, the group email box makes it difficult to tell which DIBP staffer serviced the request.

Future flows

With the FVS, every request to match or search for biometric information will be logged at the hub and identified by username of the requesting AFP officer. Most data will be passed straight through the hub, with some formatting transformation, but no addition or subtraction of Personal Information. The overall volume of biometric information flowing may increase over time as a result of the FVS but the flows will be more accountable.

Note that every request to match or search for biometric information will be logged at the hub, with indications of the requesting AFP officer, and the officers or automatic systems as applicable that fielded the inquiry at DIBP. Most data will be passed straight through the hub, with some automated data reformatting, but no addition or subtraction of Personal Information.

There will also be strict enforcement of the NFBMC participation business rules; in particular that interagency arrangements be in place to authorise use of the hub. In principle, it should be possible to use access control sub-systems in the hub to revoke access in the event that a participating agency fails a periodic privacy or security audit, or otherwise fail to comply with AGD requirements. Individual user level access control (such as blacklists or IP address white lists) could also be used without major modification to the architecture.

High level privacy analysis

Before detailed assessment against the APPs in the next chapter, we summarise the major issues as seen by Lockstep.

NFBMC privacy & security framework

The privacy of the FVS system rests on a number of security and data protection measures laid out in the FVS Access Policy [1]. Here we summarise and annotate those measures.

- **Statement of Legislative Compliance** setting out the regulatory justification for the transfer of biometric data between each agency involved.
- **Privacy Impact Assessments** will be required for each agency joining the hub.
- **Management of Nominated Users** within each participating agency will be via multifactor authentication, and will be logged and auditable by username at the individual transaction level. Some minimal logging (of unique transaction ID, username, time and date) will be done at the hub; the larger share of event logging anticipated to be needed for reasonable oversight, shall be the responsibility of the agencies.
- **Security and Privacy Awareness** training will be required for all nominated agency users.
- **Auditing and Accountability**: Agencies will be required to audit their use of the FVS at least annually. AGD's intention is to require audits to be sufficiently detailed as to cover the time and date, the purpose, and the requesting user for each transaction.
- **Interagency Data Sharing Agreements** (IDSAs) must be established between all pairs of agencies using the FVS. AGD plans to provide a template IDSA.
- **Transparency**: the PIAs , data sharing agreements (ISDAs) and the statement of legislative compliance will all be published, to the greatest extent possible, allowing for security or other reasons preventing full publication
- **Security Accreditation**, against the PSPF and ISM, of all systems connected to the hub.
- **Service Level Agreement** with the Attorney-General's Department.

Assessment against the APPs

In this section we examine the compliance of the NFBMC FVS *Match* and *Search* functions with the 13 APPs.

APP 1: Open and transparent management of Personal Info

Assessment & Findings

The AFP's use of biometric face image data at present and in the intended use of the FVS fall under the law enforcement provisions of the Privacy Act. The AFP Privacy Policy [8] provides a comprehensive account of the Personal Information and Sensitive Personal Information (including facial images and fingerprints) that the AFP may collect and why, and a list of many of the legislative mechanisms that apply, including the AFP Act [22], the *Crimes Act 1914* (Cth), the *Crimes Act 1900* (ACT) and so on.

DIBP has practices and procedures to ensure compliance with the requirements of all APPs, including APP 1 which requires a clearly expressed and up-to-date Privacy Policy about how Personal Information is managed. The Privacy Policy details how DIBP manages the Personal Information it collects and the information flows associated with that Personal Information. The Privacy Policy informs individuals how they may lodge a complaint if they believe DIBP has wrongly collected or handled their Personal Information. DIBP maintains a privacy notice, Form 1442i, *Privacy notice* [26], which includes matters required under APP 1 and APP 5 of which DIBP must advise persons when collecting and sharing their Personal Information, including personal identifiers. DIBP advises that, if individuals are not satisfied with DIBP's response, they are advised that it is open to them to contact the Australian Privacy Commissioner.

DIBP also has a separate notice, Form 1243i, '*Your personal identifying information*' [27], which explains DIBP's authority to collect personal identifiers, how they may be collected, the purposes of collection and the purposes for which they are permitted to be disclosed.

Forms 1243i and 1442i are publicly available on the Department's website.

We find that the above existing transparency mechanisms at DIBP and the AFP are not materially impacted by the introduction of the FVS hub system.

While the FVS will increase accountability of biometric information flows between DIBP and the AFP, we acknowledge prima facie privacy concerns amongst members of the public regarding biometrics and the stated concerns of privacy advocates, and thus we advise AGD to consider additional transparency measures to provide comfort to members of the public.

Recommendations

Recommendation 1. AGD should consider creating a privacy statement specific to the FVS hub, to address generally recognised privacy concerns around biometrics (such as the limits to sharing of biometrics), and to explain to the public the major data protection properties of the NFBMC. Such a privacy statement could cover the NFBMC design philosophy, key procedural and technological data protection measures, and the high level rules, like DIBP and AFP being required to enter into a bilateral data sharing agreement, and publish this PIA.

APP 2: Anonymity and pseudonymity

Assessment & Findings

Anonymity is not generally relevant to the AFP's law enforcement related use cases. The FVS makes no change to the way AFP uses biometrics nor the applicability of anonymity or pseudonymity. Therefore APP 2 is not activated, and we make no recommendations here.

APP 3: Collection of solicited Personal Information

Assessment & Findings

The FVS hub does not solicit any information at all as such, but only passes through Personal Information of individuals in relation to whom AFP officers have requested information for specific purposes permitted by legislation. No Personal Information about members of the public persists in the FVS systems or audit logs. The individuals that are the subject of FVS transactions cannot be reasonably identified from the transaction IDs and photo hashes and therefore APP 3 is not activated in respect of collection by the hub itself.

Through its use of the FVS, the AFP will continue to collect Personal Information from DIBP as it does now for law enforcement purposes, as permitted by legislation.

Facial images used for biometric identity verification are of course *Sensitive Information* under the Privacy Act (see *Glossary* above). APP 3.4(d) enables collection of Sensitive Information without consent of the individual, by an enforcement body where that body believes that collection is reasonably necessary for, or directly related to, one or more of its functions or activities. The AFP's functions are set out in section 8 of the *Australian Federal Police Act 1979* [22]. The AFP's Privacy Policy [8] is clear about its authority under the Privacy Act and the AFP Act to collect facial images. Over time, more targeted inquiries will be made possible through use of the FVS.

DIBP collects Personal Information, including facial images, for their value in resolving identity, security, law enforcement and other immigration concerns. This information is reasonably necessary for, or directly related to, the Department's functions as listed in Section 4 of the Migration Act

and Division 5 of Part 2 of the Citizenship Act.As for present data sharing arrangements, DIBP will collect Sensitive Information and Personal Information (including a facial image to be used for biometric matching and biographic details) submitted by AFP as part of a Match or Search request. DIBP has an existing legal basis to do so under APP 3.4(d)(i), which permits it to collect Sensitive Information where it is reasonably necessary for, or directly related to, its enforcement functions under the Migration Act and Citizenship Act.

We have no recommendations to make in relation to APP 3.

APP 4: Dealing with unsolicited Personal Information

Assessment & Findings

Under the FVS, DIBP will receive unsolicited requests from AFP to provide personal information about individuals. Such requests will contain facial images and biographic information. APP 4.1 provides that if an APP entity receives personal information and did not solicit this information, the entity must within a reasonable period after receiving the information determine whether or not the entity could have lawfully collected the information under APP 3, if the entity had solicited the information. As the provided personal information (including sensitive information) can be lawfully collected by DIBP under APPs 3.1 and 3.4(d)(i), the requirements of APP 4 are met.

Under section 6 of the *Privacy Act 1988*, an entity Solicits Personal Information if it requests another entity to provide the Personal Information, or to provide a kind of information in which that Personal Information is included.

As DIBP will provide facial biometric images and biographic data to the AFP via the FVS *Match* and *Search* functions solely on a query-and-response basis, AFP will receive only Personal Information it has solicited.

The hub of course fleetingly handles Personal Information that the hub itself did not solicit, as it passes through the hub between participating agencies. The hub merely provides a conduit for passing certain Personal Information between agencies, which have signed up to the FVS Access Policy, and which must have a legal basis for handling that Personal Information regardless of the hub. The express role of the hub is to improve the oversight and accountability of exchanges of biometric data, by providing easier to use and easier to audit formal automated channels. Data retained in hub audit logs about individuals who are subject to FVS transactions is not identified, contains only an externally meaningless transaction code, and is not reasonably identifiable.

APP 5: Notification of the collection of Personal Information

Assessment & Findings

DIBP currently collects facial images and biographic data from citizenship and visa applicants as part of the application process, in accordance with

the *Australian Citizenship Act 2007* [22] and the *Migration Act 1958* [23]. At the time an individual makes one of these types of application, he/she is notified through the form of matters required by APP 5.2(b), including the types of organisations to which DIBP usually discloses Personal Information so collected. In particular, Form 1243i [27] states:

> *The department is authorised to disclose your personal identifiers and information relating to your name and other relevant biographical data to a number of agencies including law enforcement ...*

The FVS will not change the purposes for which AFP collects biometric data from DIBP, nor the way AFP uses biometric data. Instead the FVS delivers face-related data to authorised police officers in a more secure, more accountable manner. Therefore, existing notification practices by DIBP and the AFP all remain sufficient to satisfy APP 5 in the context of the FVS.

We have no recommendations to make in relation to APP 5.

APP 6: Use or disclosure of Personal Information

Assessment & Findings

In a limited sense, the hub can be regarded as *using* Personal Information, insofar is it transforms some parameters sent in as part of a request so they may be passed through to a holding agency for processing. For the DIBP-AFP use cases, no Personal Information will ordinarily be disclosed by the FVS to any entity beyond the requesting agency and the agency that receives the request.

The interagency data sharing agreement (IDSA) required between DIBP and the AFP will seek to limit the ways that Personal Information obtained through the FVS may be used, in line with the AFP's and DIBP's respective legislated functions. The IDSA will provide a mechanism for DIBP to clearly articulate (and if necessary review and revise) the circumstances under which the AFP may disclose to third parties Personal Information obtained through the FVS. Currently, manual transfer of biometric data is covered by a host of MOUs. Based on the template IDSA developed by AGD, the IDSA, in Lockstep's opinion will be a distinct improvement on these, as and when the FVS comes to supersede manual transfer.

The information that DIBP is to disclose to AFP in response to a *Match* or *Search* query constitutes *identifying information* under the *Migration* and *Citizenship Acts*, *protected information* under the ABF Act and *personal information* under the *Privacy Act*.

Citizenship

DIBP is permitted to disclose citizenship-related identifying information collected from citizenship applicants, including facial images, in a number of circumstances in connection with the express or implied purposes or objects of the *Citizenship Act*, including where the disclosure:

- is to a state/territory/commonwealth agency in order to verify that a person is an Australian citizen (s 43(2)(da))
- takes place under an arrangement entered into with a state/territory/commonwealth agency for the exchange of identifying information (s 43(2)(e)), and
- is reasonably necessary for the enforcement of a state/territory/commonwealth criminal law (s 43(2)(ea)).

Under section 6.2 (b) of the *Privacy Act*, DIBP is authorised to disclose personal information, including a facial image provided at the time of citizenship application where the disclosure is "required or authorised by or under an Australian law or a court/tribunal order". The *Australian Passports Act 2005* authorises the disclosure by DIBP to AFP of the facial image. Therefore APP 6 is satisfied.

Visa/Immigration

DIBP is permitted to disclose visa-related identifying information including facial images in a number of circumstances in connection with the express or implied purposes or objects of the *Migration Act*, including where disclosure:

- is for the purpose of data-matching in order to identify, or authenticate the identity of a person (s 336E(2)(a)(i))
- takes place under an arrangement entered into with a state/territory/commonwealth agency for the exchange of identifying information (s 336E(2)(e)), and
- is reasonably necessary for the enforcement of a state/territory/commonwealth criminal law (s 336E(2)(ea)).

Where disclosure is required or authorised by or under a law of the Commonwealth, a State or Territory (for example, Part 4A of the *Migration Act* in relation to identifying information), this will automatically comply with Part 6 of the ABF Act (paragraph 42(2)(c) of the ABF Act) and with APP 6.2(b) of the *Privacy Act*.

Where disclosure is required or authorised by or under a law of the Commonwealth, a State or Territory (for example, Part 4A of the Migration Act in relation to identifying information), this will automatically comply with Part 6 of the ABF Act (paragraph 42(2)(c) of the ABF Act) and with APP 6.2(b) of the Privacy Act 1988.

Privacy Risk: secondary use of Personal Information

In principle, there is a risk that DIBP-sourced Personal Information received via the FVS might be put to an unauthorised purpose by the AFP unrelated to the primary purpose of collection at DIBP and outside of legitimate secondary uses permitted by law enforcement exceptions under APP 6.2(e). We note that this risk is present in the current manual processes for exchanging biometric and biographical data, as described above in *Information flow mapping*.

The main mitigation of the existing risk is the commitment of the AFP to proper handling of Personal Information outlined in the agency's privacy statement and policy [7][8]. This in-principle risk is not fundamentally altered by the introduction of the FVS. This PIA, scoped to assess the introduction of the FVS, can assume that existing AFP processes are compliant with the *Privacy Act*. Having said that, the IDSA to be signed by both DIBP and AFP will further tighten information handling arrangements.

Once FVS-enabled processes are widely implemented, the risk of inappropriate secondary usage of biometric Personal Information may be somewhat reduced as a result of the superior auditability of data flows. It may be easier in future to determine where a given record came from and which authorised user of the FVS would have retrieved the record in the first place. While the subsequent flows and usage of PI are beyond the control of NFBMC and outside the scope of this PIA, the better transparency of the initial retrieval may act as an aid to the investigation of inappropriate usage, and as a deterrent too.

Nevertheless, Lockstep notes that when the ability to search biometrics holdings is enhanced, there arises the possibility of unauthorised access and use. Given the ever present risk of human failings, it is good practice for government users of database search functions to be given reminders of their obligations under employment terms and conditions to not abuse their powers.

See also *Limiting use of the hub* in the main body of the report.

Privacy risk – disclosing unsolicited information

On rare occasions, a false match of a probe image against DIBP's holdings will result in Personal Information being provided to the AFP that may not be about the person of interest. The matching requirements of the service require that the biographic details of the probe and the falsely matched image would have to match, making this occurrence highly unlikely. We assume that in practice, the rate of such occurrences will be reduced to negligible levels by the tuning of the system false match and false non-match performance.

Recommendations

Recommendation 2. The FVS portal, at the time that a *Match* or *Search* is requested, should display a reminder to users of their obligations as officers of AFP to treat all Personal Information in accordance with the Privacy Act and other relevant terms of their employment conditions.

APP 7: Direct marketing

Assessment & Findings

Direct marketing is not applicable. Therefore APP 7 is not activated for the purposes of this PIA.

APP 8: Cross-border disclosure of Personal Information

Assessment & Findings

Any cross-border flow of Personal Information in the anticipated operation of the FVS by AFP will be to locations under full control by the AFP, using systems and processes that comply with the APPs. Thus APP 8 will be satisfied.

In theory, there is a risk that DIBP-sourced Personal Information might be transmitted across borders to a country that does not comply with the APPs. The same risk is present in the current manual processes for the retrieval by AFP from DIBP of biometric and biographical data. The main mitigation of that risk is AFP's commitment to proper handling of Personal Information outlined in section 6(a) of the AFP Privacy Policy [8] and the IDSA that will govern disclosure of information by DIBP to the AFP. This risk is not fundamentally altered by the introduction of the FVS and since this PIA focuses on the impact of the introduction of the FVS, we may assume that existing AFP processes are compliant with the Privacy Act.

We make no findings or recommendations with respect to APP 8.

APP 9: Adoption, use or disclosure of government identifiers

Assessment & Findings

APP 9 applies to adoption, use or disclosure of government identifiers by an "organisation", which is defined in section 6C of the *Privacy Act* to exclude an "agency". Under s 6 of the *Privacy Act*, an "agency" includes a Department. Therefore, neither AFP nor DIBP are organisations for the purposes of the Privacy Act, and APP 9 does not apply to AFP's and DIBP's adoption, use or disclosure of government identifiers.

Thus we find that APP 9 will not be activated by the use of the FVS *Match* and *Search* by DIBP and AFP, and so we make no findings or recommendations with respect to APP 9.

APP 10: Quality of Personal Information

Assessment & Findings

The FVS plays no direct part in the quality of biometric data holdings at any agency. In respect of APP 10, the FVS hub is neutral.

It could be argued that the use of the FVS should, over time, lead to improved quality in biometrics holdings, through better detection of discrepancies and more targeted usage. It is difficult to generalise at this time and we leave it to other agency-specific PIAs in future, under the NFBMC participation arrangements, to evaluate the possible improvements to quality that the hub might facilitate.

Any personal information obtained by the AFP from DIBP through the FVS will be subject to the agency's existing obligations to take reasonable steps to ensure the quality of personal information they use or disclose. In addition to existing procedures for discharging this obligation, based on the requirements of the Access Policy and the IDSA template, the IDSA [2] between AFP and DIBP will contain express protections that apply to secondary use of Personal Information obtained under the new data sharing arrangements. AGD advises that these protections would require AFP to take reasonable steps to confirm the accuracy of the information with DIBP through other means, before using the information for evidentiary or other purposes. This mechanism in the IDSA would reinforce existing obligations under the Privacy Act to ensure the quality of Personal Information collected by the AFP.

We have no recommendations regarding APP 10.

APP 11: Security of Personal Information

Assessment & Findings

We understand that the FVS has been subject to standard risk assessment, as a matter of course, and will be reviewed by an IRAP assessor and approved by the AGD IT Security Advisor in accordance with the ISM. A condition of the FVS Access Policy is that DIBP and AFP systems also be IRAP-assessed. With Personal Information only transiting the system (not remaining in the system) and following pathways that are better defined and controlled than the current manual biometric handling processes, Lockstep considers that the security of Personal Information should be much enhanced by the FVS.

Auditing

When a *Match* or *Search* request is sent to the FVS hub, details of the request and its results are recorded in an audit log at the hub (see *Audit Information,* [12][13][14][15]). The audit log records the following:

- *Transaction ID & Group ID*
- *Requesting Agency, User Name and System Name*
- *Function Accessed (e.g. Match, Search)*
- *Transaction Message Status Code*
- *Date and Time of Match Request Receipt*
- *Search Request Type*
- *Date and Time of Match Request Response.*
- *Unique identifier of response record(s); and*
- *Message (if provided).*

In Lockstep's opinion, these details are moderate in the context of FVS usage, and therefore are in keeping with APP 3. We note that no Personal Information about members of the public is logged.

While the auditing is moderate, we note in the context of APP 11 that the details may actually be found to fall short. In the event of a dispute or

other event after the fact, related to a NFBMC transaction, there may be interest in the exact configurations of the past matching performed. Such details are not retained at the hub, and should never be retained according to the NFBMC philosophy. We do not recommend changing the philosophy but we do advise that participating agencies be reminded (perhaps in the IDSA guidance) of the need to consider local logging of greater detail of the biometric matching procedures.

Access control

Access control measures provided under DIBP's IDSA with the AFP [2] will mitigate against misuse and unauthorised access, modification or disclosure by requesting agency staff. As noted in the section on training and management of FVS users, access to the FVS will only be provided to nominated AFP users, restricted to employees who have a reasonable need to use the FVS to fulfil their employment functions. In accordance with the FVS Access Policy, the AFP will be required to maintain registers of nominated users for oversight and auditing purposes. Audits will be undertaken annually and will examine records that identify the time, purpose and nominated user associated with each transaction. These records will provide the ability to detect any anomalous or potentially suspicious transactions. These oversight measures will provide a strong deterrent for misuse of personal information by AFP users.

From our review of the architecture, it appears possible in principle to use access control sub-systems in the hub to revoke access in the event that a participating agency fails a periodic privacy or security audit, or otherwise fail to comply with AGD requirements. Individual user level access control (such as blacklists or IP address white lists) could also be used without major modification to the architecture, to provide additional active protection against abuse by ex-employees.

Recommendations

- **Recommendation 3.** Ensure that the AFP and DIBP understands the limited event logging of the hub, and the need to cater for its own logging and auditing requirements. In particular, ensure that AFP and DIBP system designers understand that biometric algorithm and matching parameters are not retained by FVS and may not be made available by FVS if ever needed.

- **Recommendation 4.** AGD should consider adding advice to the IDSA guidance that requesting agencies (AFP in this case) locally record details from time to time of the biometric algorithms used by the holding agency (DIBP here), in case future investigations of, for example, false matches, need to reference the algorithms and parameters applied in each usage of the FVS.

- **Recommendation 5.** The AFP should retain its own records of all biometric matching parameters and other configuration information (algorithms, biometric product version numbers etc.) used by DIBP to produce each *Match* or *Search* result. Algorithm updates,

especially changes to threshold parameters used for matching or searching, will change the performance of the processes from time-to-time, and these changes should be tracked by the AFP, so that in the event that a dispute arises, the precise conditions of past matches are not lost.

APP 12: Access to Personal Information

There is no Personal Information retained in the FVS about individual members of the public who are the subject of transactions, only transaction IDs held in the audit logs that are meaningless outside separate participating agencies (plus the usernames of the authorised agency users involved in the transactions). There is no Personal Information in the system at all to which a member of the public could, in principle, have a right to access under APP 12.

We find that APP 12 is not activated and therefore we make no recommendations.

APP 13: Correction of Personal Information

Assessment & Findings

Further to the APP 12 assessment above, APP 13 is not activated by the FVS. It may be noted that by improving and formalising the use of biometric matching between agencies, the FVS (and NFBMC more broadly) has some potential to improve compliance with APP 13 by participating agencies.

Conclusions

We conclude that the Face Verification Service – as exemplified by the AFP-DIBP use cases for *Match* and *Search* – should bring an important addition to the exchange of biometrics and personal information to law enforcement while maintaining the privacy of biometric data processed by government agencies. Facial biometric data is a critical asset for managing national security and combating fraud. It is a reality that biometric data will be used more widely and more deeply in coming years. It is timely therefore that the FVS be introduced, chiefly as a means to facilitate the real-time flow of facial data and related personal information and personal identifiers between government agencies, supplementing existing manual processes in the circumstances under which it will occur.

Lockstep finds that the NFBMC is likely to improve privacy in the data sharing arrangements between DIBP and the AFP, by avoiding unnecessary manual handling of, and exposure to, biometric data by data holding agencies, and specifying the FVS functions that can be accessed by agencies and named staff members who meet stringent security and privacy requirements as set out in the FVS access policy.

Recommendations

1. AGD should consider creating a privacy statement specific to the FVS hub, to address generally recognised privacy concerns around biometrics (such as the limits to sharing of biometrics), and to explain to the public the major data protection properties of the NFBMC. Such a privacy statement could cover the NFBMC design philosophy, key procedural and technological data protection measures, and the high level rules, like DIBP and AFP being required to enter into a bilateral data sharing agreement, and publish this PIA.
2. The FVS portal, at the time that a *Match* or *Search* is requested, should display a reminder to users of their obligations as officers of AFP to treat all Personal Information in accordance with the Privacy Act and other relevant terms of their employment conditions.
3. Ensure that the AFP understands the limited event logging of the hub, and the need to cater for its own logging and auditing requirements. In particular, ensure that AFP system designers understand that biometric algorithm and matching parameters are not retained by FVS and may not be made available by FVS if ever needed.
4. AGD should consider adding advice to the IDSA guidance that requesting agencies (AFP in this case) locally record details from time to time of the biometric algorithms used by the holding agency (DIBP here), in case future investigations of, for example, false matches, need to reference the algorithms and parameters applied in each usage of the FVS.
5. The AFP should retain its own records of all biometric matching parameters and other configuration information (algorithms, biometric product version numbers etc.) used by DIBP to produce each *Match* or *Search* result. Algorithm updates, especially changes to threshold parameters used for matching or searching, will change the performance of the processes from time-to-time, and these changes should be tracked by the AFP, so that in the event that a dispute arises, the precise conditions of past matches are not lost.

References

Project documents

[1]. *Face Verification Service (FVS) Access Policy* v5.3 Attorney-General's Department
Filename: Meeting paper - Item 2(d) - Attachment A - Facial Verification Service Access Policy - Programme Advisory Committee - 7 April 2016.docx

[2]. *Interagency Data Sharing Agreement* [template] V3.1, 24 March 2016 National Facial Biometric Matching Capability Face Verification Service
Filename: Meeting paper - Item 2(d) - Attachment B - FVS IDSA template - Programme Advisory Committee - 7 April 2016.docx

[3]. *Interoperability Hub Technical Concept of Operations*, Attorney-General's Department, October 2015
Filename: Technical Concept of Operations.docx

[4]. *Face Matching Services*, (undated), Attorney-General's Department
Filename: Fact-Sheet-National-Facial-Biometric-Matching-Capability.pdf

[5]. *Identity Hub: System Access Flows*, Draft v0.4 April 2015
Filename: MASTER - AGD Access Maps DRAFT v0.4.pdf

[6]. *National Facial Biometric Matching Capability Privacy Impact Assessment – Interoperability Hub*, Information Integrity Solutions, August 2015
https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Privacy-Impact-Assessment-National-Facial-Biometric-Matching-Capability.PDF

[7]. *Australian Federal Police Privacy Statement*
www.afp.gov.au/global/privacy

[8]. *AFP Privacy Policy*
http://www.afp.gov.au/~/media/afp/pdf/a/afp-privacy-policy-001.pdf
(accessed 11 April 2016)

[9]. *Concept of Operations National Facial Biometric Matching Capability* v0.7
Filename: Concept of Operations - National Facial Biometric Matching Capability - .pdf

[10]. *Blueprint National Facial Biometric Matching Capability* (undated),
Filename: Master Blueprint - National Facial Biometric Matching Capability - Nov 2...pdf

[11]. *Inter-Operability Hub (IOH) System Specification (Pilot)*, v1.0, Dinesh Kotni, DIBP Client Services and Identity (CSI), March 2016

[12]. '*Verification -> Match Function - DIBP Citizenship Data* v0.4.1, Michael Fox, Attorney-General's Department, 4 August 2016
Filename: Interoperability Hub - Verification - Match Function - DIBP Citizenship ....docx

[13]. '*Verification -> Search Function - DIBP Citizenship Data* v0.4.1, Michael Fox, Attorney-General's Department, 4 August 2016
Filename: Interoperability Hub - Verification - Search Function - DIBP Citizenship....docx

[14]. '*Verification -> Match Function - DIBP Visa Data* v0.8.1, Michael Fox, Attorney-General's Department, 4 August 2016
Fileneme: Interoperability Hub - Verification - Match Function - DIBP Visa Data FO....docx

[15]. '*Verification -> Search Function - DIBP Visa Data* v0.7.1, Michael Fox, Attorney-General's Department, 4 August 2016
Fileneme: Interoperability Hub - Verification - Search Function - DIBP Visa Data F....docx

[16]. *Privacy Impact Assessment: DFAT Access to DIBP Face Verification Service (Retrieve Function) for Citizenship Images [Report 1]* V1.2, Lockstep Consulting, March 2016

[17]. *Privacy Impact Assessment: AFP Access to DIBP Face Verification Service (Retrieve Function) for Citizenship Images [Report 2]* V1.0, Lockstep Consulting, June 2016

[18]. *Basis for DIBP to disclose Identity Information to DFAT AFP*, Duncan Anderson, Attorney-General's Department, by email, 19th January, 2016.

[19]. *DIAC Project Privacy Impact Assessment*, Dept of Immigration and Citizenship Identity Branch, 11 November 2009
Filename: DIAC DFAT Exchange of Identity Data Part A - PIA v0.13

[20]. *Draft IPP Audit Report: DIAC Exchange of identity data through the Systems for People project*, Office of the Privacy Commissioner, March 2010
Filename: Audit - 2010-03 DIAC SfP Draft Audit Report amac.doc

External References

[21]. *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)*

[22]. *Citizenship Act 2007 (Cth)*
http://www.austlii.edu.au/au/legis/cth/consol_act/aca2007254/

[23]. *Migration Act 1958 (Cth)*
http://www.austlii.edu.au/au/legis/cth/consol_act/ma1958118/

[24]. *Australian Federal Police Act 1979 (Cth)*
http://www.austlii.edu.au/au/legis/cth/consol_act/afpa1979225/

[25]. *Australian Border Force Act 2015 (Cth)*
http://www.austlii.edu.au/au/legis/cth/num_act/abfa2015225/

[26]. *Privacy notice* form 1442i, Department of Immigration and Border Protection
https://www.border.gov.au/Forms/Documents/1442i.pdf

[27]. *Your personal identifying information* form 1243i, Department of Immigration and Border Protection
https://www.border.gov.au/Forms/Documents/1243i.pdf

[28]. *Australian Privacy Principles guidelines*, Office of the Australian Information Commissioner, V1.0, February 2014
http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf

[29]. *Martin Place Siege: Joint Commonwealth - New South Wales review,* Department of Prime Minister and Cabinet, and NSW Premier and Cabinet, January 2015
https://www.dpmc.gov.au/sites/default/files/publications/170215_Martin_Place_Siege_Review_1.pdf

[30]. *New $18.5 million biometrics tool to put a face to crime,* Minister for Justice, Media Release, 9 Sept 2015

[31]. *Document Verification Service Privacy Policy*
http://www.dvs.gov.au/Pages/Disclaimers/Privacy-statement.aspx
(accessed 14 Jan).