Document verification service

Consultation paper for privacy impact assessments for proposals to enhance the document verification service

22 January 2013

Request for assistance from AGD

The Australian Government Attorney-General's Department (AGD) has commissioned Clayton Utz to prepare reports scoping the potential privacy impacts of proposals to enhance the availability and functionality of the national Document Verification Service (DVS) in terms of recent Commonwealth privacy reforms. The proposals involve both privacy risks and benefits. To develop the privacy impact assessments, AGD seeks your assistance in identifying these risks and benefits, as well as potential controls or mitigation strategies.

To this end, AGD has asked Clayton Utz to conduct targeted consultation with key stakeholders related to the Commonwealth components of the service. This paper is intended to provide a brief overview of the proposals to assist in the consultation process.

The consultation process, and how you can assist, is set out in the next steps section of this paper (on page 5).

Contents

Background—What is the DVS?

AGD manages the DVS on behalf of all Australian governments. The DVS is a key element of the National Identity Security Strategy endorsed by the Council of Australian Governments.

The DVS is a secure online system that enables organisations to verify information on a customer's evidence of identity documents with the records of the document issuing agency.

The DVS currently provides organisations with the ability to verify information on a range of evidence of identity documents issued by Australian Government and state and territory government agencies. These include immigration documents, passports, driver licenses, Medicare cards as well as birth, marriage, and change-of-name certificates.

The DVS is not a database. DVS transactions involve a check of whether the information presented on an evidence of identity document matches the records of the issuing agency. The results are provided in the form of a 'yes/no' result. DVS checks must be undertaken with the informed consent of the person whose information is being used, and no personal information is retained following the completion of a check.

DVS checks have been available to by government agencies since 2009, and (with the exception of birth, marriage and change of name data) are now being made available to the private sector, with an initial focus on organisations that have legislative obligations to identity their customers. For example, financial institutions which need to meet 'know your customer' requirements in anti-money laundering and counter-terrorism financing regulations.

Any organisation using the DVS is required to comply with the *Privacy Act 1988* (Cth) or any relevant state and territory privacy legislation.

For further information on the DVS see www.dvs.gov.au.

Proposals to expand the functionality and availability of the DVS

AGD is considering two proposals which are set out below. In addition, some of the privacy risks and benefits which have already been identified are set out.

1 Expanded commercial access: Reforms to the Privacy Act 1988 will come into effect in March 2014 which include amendments to use by organisations of Commonwealth government identifiers (previously dealt with by NPP 7.2). The new APP 9.2 allows use of government identifiers by organisations in different circumstances, including where 'the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions.'

The current DVS access management policy (see the Attachment at page 6) limits commercial access and use to businesses operating under legislated client identification requirements. This restriction was informed by the prohibitions and permissions of the Privacy Act 1988 (NPPs 7.2, 2.1). In light of privacy reforms AGD is reviewing DVS access policies and is considering in particular potential privacy risks in expanding the range of businesses eligible for DVS access as may be permitted under the APPs.

Potential privacy issues, risks and benefits:

- Defining the circumstances in which use of an identifier is "reasonably necessary" for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions
- Facilitating online transactions without the need for hardcopy identity documents to be provided
- Limiting use by organisations to circumstances only where there is a reasonable need to verify the identity of the individual for the organisation's activities or functions
- Avoiding more intrusive identity verification methods, for example avoiding the need for organisations to keep copies of identity documents

2 **Expanded functionality (field specific matching):** DVS technical functionality currently provides a one character response indicating the cumulative accuracy of all data fields used to match a document – a confirmed match (Y) response indicates that all five fields completely match. Negative responses provide no information as to why an N result is returned.

The challenge of translating the complexity of some identity documents into DVS match requests can result in inaccuracy at the data entry stage and the return of false 'N' responses. This can result in Users resubmitting queries until a Y result is returned, generating multiple unnecessary N results and additional traffic through the system.

Field specific matching (FSM) could assist Users to minimise the number of repeat match requests by providing a code from the Issuer indicating formatting errors or fields that were not matched in the search. Both public and private sector Users have indicated a strong interest in such a capacity.

An FSM code would simply refer the User back to a specific field on the identity document for re-examination. AGD anticipates that FSM could deliver considerable service improvements to organisations and their customers by limiting the degree of guesswork in DVS requests, reducing the amount of retried queries, minimising the time taken to gain an accurate result, and improving customer service.

Potential privacy risks and benefits:

- Avoid unnecessary false negatives due to input error
- Improve identity decision-making by providing Users with information to start a discussion with a customer
- FSM could reduce the amount of information which is necessary for the purposes of verifying an identity
- Whether there are other ways in which false negatives could be avoided without FSM

Privacy impact assessments into the proposals

AGD has instructed Clayton Utz to prepare two privacy impact assessments in relation to the two proposals discussed.

► Report A—Privacy impact assessment of expanded private sector access

We are instructed to prepare a Privacy Impact Assessment (PIA) identifying privacy impacts and options to mitigate any privacy risks related to extending use of the DVS to private sector organisations in the context of the national privacy regime set out in the *Privacy Act 1988*, as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

Report A will:

1) assess the privacy risks associated with expanding the range of businesses able to use the DVS for the purposes of verifying information on government issued identifiers to include any organisation with a 'reasonable necessity' to identify an individual as per Australian Privacy Principle (APP) 9.2(a)

2) assess any privacy benefits that may accrue from wider private sector use of the DVS, as an alternative to other methods of verifying government issued identifiers that are commonly used by private sector organisations, and

3) identify options to mitigate any privacy risks associated with expanded private sector use of the DVS.

In doing so the report will need to take into account:

- the draft PIA material prepared by AGD
- existing privacy and information security measures including contractual terms and conditions on DVS private sector access; existing privacy, information security, and business rules of the DVS, and
- governance processes for DVS private sector access.

Preparation of the report will include consultations with a range of Commonwealth government and non-government stakeholders such as:

- Commonwealth document issuing authorities – Department of Foreign Affairs and Trade, Department of Immigration and Border Protection, Department of Human Services;
- DVS User organisations – government and business;
- The Office of the Australian Information Commissioner – the Privacy Commissioner, and
- Non-government privacy advocates (Australian Privacy Foundation, Liberty Victoria, Electronic Frontiers Australia)

Report B—Privacy Impact Assessment of Enhanced DVS Functionality (field specific responses)

We are instructed to prepare a Privacy Impact Assessment identifying privacy impacts and options to mitigate any privacy risks related to enhancing the DVS to return responses indicating the specific data field(s) that did or did not verify. The report will consider these impacts in the context of the proposed expansion of DVS private sector access (Report A).

Report B will:

1) assess the privacy risks associated with the enhanced DVS functionality providing data field specific responses,

2) assess the privacy benefits associated with enhanced DVS functionality, and

3) identify options to mitigate any privacy risks associated with the enhanced DVS functionality.

In doing so the report will need to take into account:

- Report A: Privacy Impact Assessment of Expanded Private Sector Access
- draft business model material prepared by AGD
- existing privacy and information security measures including contractual terms and conditions on DVS private sector access, existing privacy, information security, and business rules of the DVS, and
- governance processes for DVS private sector access.

Preparation of the report will include consultations with a range of Commonwealth government and non-government stakeholders such as:

- Commonwealth document issuing authorities – Department of Foreign Affairs and Trade, Department of Immigration and Border Protection, Department of Human Services
- DVS User organisations – government and business
- The Office of the Australian Information Commissioner – the Privacy Commissioner, and
- Non-government privacy advocates (Australian Privacy Foundation, Liberty Victoria, Electronic Frontiers Australia)

Next steps—how you can help

We intend to hold face-to-face or teleconference consultation sessions in the week of 10 February 2014. The face-to-face sessions would be held in Canberra, Sydney and Melbourne depending on need and availability. To better inform those sessions, it would assist us to know your initial thoughts about the proposals. We have set out in the following section the questions which on which we would appreciate your thoughts. Following the consultation sessions, we anticipate that you may wish to flesh out or amend your written submissions. We are therefore proposing to ask for final written submissions, following the consultation sessions, by 28 February 2014.

Proposed consultation timetable

Initial written comments — By 7 February 2014

Consultation sessions (face-to-face or teleconference) —Week of 10 February 2014

Final written submissions — By 28 February 2014

Questions for consultation

Generally:

- Without the DVS, what other methods (paper-based, electronic, etc) can organisations use to verify the identity of individuals?
- What might be the downstream privacy impacts of those other identification processes (document copying, record keeping, etc)?

In relation to each proposal:

- What impact do the amendments to the *Privacy Act 1988* (Cth) have on the lawfulness of the proposal?
- In what circumstances could the proposal have a positive impact for individuals whose identities are being verified by an organisation?
- In what circumstances could the proposal have a negative impact for individuals whose identities are being verified by an organisation?
- In what ways can any negative impacts could be managed?
- What security or access controls should be adopted if the proposal is adopted?
- What information should individuals be given about the results from the DVS if the proposal is adopted?

Please also address any other issues you see with the proposal.

Attachment— Policy for access to the Document Verification Service by Business Users

The nationally agreed policy for the commercial DVS limits its use to businesses with legislated identification obligations. In consultation with national stakeholders, AGD is exploring the potential for expanded private sector use, initially as it might align with the recent reforms to the Commonwealth privacy regime.

Access policy context

In the first phase of extending access to DVS to the private sector, it will be provided to entities that have a client identification requirements under Commonwealth legislation. Government already regulates the operations of these agencies. Access to the DVS will take account of these existing risk-based regulatory procedures. Given all governments' stated objective is to reduce red tape for industry, DVS represents a method that can potentially streamline and reduce these regulatory burdens, rather than creating new procedures. Examples of regulatory authorities that oversee likely DVS users are:

- ACMA
- Austrac
- APRA
- Office of Transport Security
- OAIC (including the Privacy Commissioner)
- ASIC

Business Users must also be subject to the privacy regime set out under the National Privacy Principles and the Privacy Act 1988.

Principles for access

The DVS is a commercial service and will operate on commercial lines. DVS Business User Applications will be accepted on a 'first-come, first-served' basis. Private sector organisations applying to become an approved DVS Business User need to meet the following requirements:

1. are subject to the Privacy Act 1988,
2. have a demonstrable requirement under law to verify the identity of their clients
3. are employing the DVS for an appropriate use, e.g. client registrations
4. operate within a regulatory regime, e.g. a banking or financial service licencing schemes in the case of financial institutions.
5. will agree to comply with all DVS private sector requirements, e.g. obtaining the informed consent of their clients, ICT and information security controls, logging and monitoring use, compliance reporting and audits etc. , and
6. will agree to undergo independent audits of their use of the DVS

Where the DVS Advisory Board does not have a specific and material objection to the organisation and the organisation pays the applicable fees at the time of application, it will be approved as a DVS Business User.