Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

15 February 2013

Mr Andrew Rice
Assistant Secretary – Cyber and Identity Security Policy
National Security Resilience Policy Division
Attorney-General's Department

Dear Mr Rice

Re: Consultation re DVS Extension Project

I refer to previous correspondence in late 2012 on this matter, conducted over the signature of the APF's Chair, Roger Clarke.

Due to the emergence of a potential conflict of interest, Dr Clarke will no longer be taking any active role in this matter.

I apologise for the delay in responding, and hope that it will still be possible to accept our input. I attach a submission by the APF on this project.

We would appreciate your acknowledgement of receipt, and your substantive response in due course.

We look forward to a constructive dialogue on the matter.

Thank you for your consideration.

Yours sincerely

David Vaile
Vice-Chair, for the Board of the APF
0414 731 249, d.vaile@unsw.edu.au

Australian Privacy Foundation

Submission relating to the DVS Extension Proposal

February 2013

Background

The Document Verification System (DVS) is a scheme operated by the Department of Human Services (DHS), under supervision by the Attorney-General's Department (AGD), and under a Council of Australian Governments (COAG) arrangement, to enable specific government agencies to check personal data against other agencies' databases. It has been operational since 2007, and was the subject of a previous internal Privacy Impact Assessment (PIA) process at that time.

A proposal has been developed over a period of years to extend the scheme in at least three ways:

- to permit some categories of corporations – perhaps 17,000 in all – to use the scheme;
- to permit corporations to act as agents on behalf of government agencies and corporations;
- to enable access to the Medicare database to verify Medicare cards/numbers.

The proposal had been articulated to a reasonably detailed level by late 2011. A PIA was commissioned from IIS Consultants in early 2012. Consultations were held with agencies, with State and Territory governments, and with corporations and industry associations.

No consultations were held with any organisations representing the interests of the affected public. A PIA Report was submitted by IIS in July 2012.

The PIA Report recommended that consultations be held with relevant public advocacy organisations if any further extension was considered (p. 32). But it failed to recommend that any consultation be conducted in relation to the present proposal.

Even after the PIA Report was published, no consultation was conducted. Moreover, the PIA Report was suppressed. As a result of an FOI request, the PIA Report was published in mid-October 2012. Only in late October 2012 was the existence of the PIA Report, and hence of the DVS Extension Proposal, communicated to public interest advocacy organisations.

The Australian Privacy Foundation (APF) expressed serious concern to AGD about the development of such a significant proposal in the complete exclusion of organisations that represent the public interest in such matters. AGD agreed on 30 November 2012 that "we undertake to consider [the APF's views] in our planning for offering the existing DVS service to the private sector".

This document is the APF's submission in relation to the matter. The APF understands that AGD will consider this document, provide its response, reflect APF's views in its further planning, directly involve APF in the project, and implement agreed modifications and enhancements.

The Published Information

The information available to APF about the DVS Extension Proposal is limited to the following:

- the description of the current DVS scheme in Appendix 2 (pp. 35-44) of the PIA Report of July 2012;
- the description of the DVS Extension Proposal on pp. 13-20, and in Appendix 3, p45 of the PIA Report of July 2012;
- the analysis of privacy impacts on pp. 21-32, and in Appendix 5, pp. 47-57 of the PIA Report of July 2012.

AGD's letter of 14 December 2012 affirmed that "The description of the [DVS scheme and the DVS extension proposal] as provided in [that PIA Report] has not changed". We understand from AGD that these descriptions encapsulate accurate and comprehensive information, and renders unnecessary any resort to the previous PIA Report or to any other source.

The following section presents the APF's analysis, followed by its submissions.

1. Misleading Statements

A considerable number of statements are made in the descriptions of both the current scheme and the proposed extension that are misleading, some seriously so.

(a) Identity Credentials

Continual reference is made to 'identity credentials'. This is correct in relation to passports.

APF disputes that any of the other agencies issue "identity credentials", in that:

- a visa attests to an attribute of the holder of a (foreign) passport;
- driver licensing authorities issue licences for a very narrow range of purposes related to the administration of traffic laws, not as a general-purpose 'identity credential';
- registrars of births, deaths and marriages record events, and issue documents that attest to the existence of an entry in a register; they do not issue 'identity credentials'.

The fact that other documents are often used as ‘evidence of identity’ and that the DVS scheme seeks to facilitate such use is no reason to inaccurately describe them.

(b) 'Presentation of the Document'

At multiple points, there are assertions and implications that the individual presents the document to the applying agency. For example, "The message information attached to a verification request provides information to an Issuer Agency that an EOI document has been presented for verification" (p. 44).

This error is repeated in the section relating to the proposed extensions, e.g. "a User Organisation seeks confirmation from an Issuer Agency ... that a document presented is valid" (p. 14).

In a great many circumstances, this is simply wrong.

More appropriate formulations are also used, e.g. "the personal information used in the DVS is provided by the individual, and in the case of online applications they might themselves enter the details into the system" (p. 43), and "in most cases, individuals will not need to present documents" (p. 14).

This is a matter of great importance. There are already many circumstances in which the document is not presented, and the data may therefore not be drawn from the document. These include:

- where the individual keys the data into an online system, or provides it by telephone
- where the requesting agency transfers from the data from its own system

(c) The Meaning of Matches and Failed Matches

The matching is based on equivalence between the data sent by the requesting agency and the data held on file by the reference agency, based on a set of comparison rules.

It is vital that requesting agencies understand the specific meaning of the 'YES', 'NO' and 'ERROR' messages that are transmitted back to them, and not misinterpret their meaning.

The meaning is emphatically not that "the document has been verified" (pp. 39-40).

APF understands the meanings to be:

YES means 'the data sent by the requesting agency was successfully matched with the data held on file by the reference agency, based on a set of comparison rules'.

NO means the above statement is not true, but no inference can be drawn as to whether the problem was with the data sent by the requesting agency, the data held by the reference agency, and/or the comparison rules

ERROR means that the request could not be fulfilled, due to technical reasons, and no inferences can be drawn in relation to what the result would have been had it been technically possible to fulfil the request

(d) Consent

At multiple points, reference is made to DVS being "a consent-based" scheme, and to "authorisation from the applicant to undertake checks".

In relation to many, and possibly all, uses this is at least misleading and arguably simply false.

Individuals are required to provide designated information to agencies, under authority of law, as a condition of applying for various registrations, services and benefits.

Agencies have authority to cross-check that information.

It is a fundamental requirement of a consent that it be freely-given, informed and granular.

It is a serious misrepresentation for any agency to create a pretence that an individual is providing consent when there is no choice in the matter, and it is therefore not freely-given.

The PIA Report (p. 21) is seriously deficient in that it accepts the inappropriate assumption that the current operation of the DVS is based on informed consent.

Further, the PIA Report is seriously deficient in carrying over the same spurious argument in relation to use by corporations as part of the DVS Extension Proposal.

(e) 'Identical Information'

At multiple locations, there is reference to the data provided by the applying agency having to be identical to that held in the database of the reference agency.

On the basis of Appendix 4, this is false. It appears that:

- "birth date ... can either be full or partial format"
- family name may differ because of the length of implementing fields
- given name is said to be singular, whereas documents and systems may carry more than one
- given name may differ because of the length of implementing fields
- middle name is optional

No information is provided about presentation-variants and spelling-variants, which is particularly important in relation to:

- embedded spaces and hyphens
- names that have been transliterated from non-Roman scripts

- names that have optional components (such as saints or prophets of the individual's religion)
- names that have different structures or sequences from conventional anglo names (such as placement of Chinese Family Names first)
- names that may or may not include a localised variant, e.g. AsianFamilyName {LocalName} AsianGivenName1 AsianGivenName2 Lee {Tommy} Gwan Fing

(f) Related Purpose

It is asserted that the use "to confirm whether the information on the EOI document corresponds to the record held on the document issuer agency's database" is "consistent with the purpose for which the information was collected" (p. 43).

This is simply a corruption of the concept of 'purpose of collection'.

Data is collected by each reference agency in order to fulfil the functions of that agency. As discussed in 1(a) above, only the passport is in any sense designed as a formal identity document, and the purposes of a passport are tightly circumscribed.

In respect of all other agencies, the use for matching against data from other agencies is an extraneous purpose, and must be subject to either consent or specific legal authority.

As discussed in 1(d) above, the circumstances are such that no consent exists.

It is therefore essential that all uses be subject to explicit legal authority, and not excused on the spurious basis put forward in the description.

(g) Extent of the Legal Authority

The DVS extension proposal is predicated on "a demonstrable legal obligation to identify people" (p. 13, repeated on p. 17).

This is materially different from, and weaker than, "an explicit legal authority for the organisation to provide information to a reference agency and to receive a response", which is what we argue is required to provide a lawful basis for the uses and disclosures involved.

2. Inadequate Transparency

(a) Unpublished Documents

The following documents are referred to, and appear to contain information of relevance to the evaluation, but have not been provided:

- MoUs between federal applying agencies and federal reference agencies
- relevant aspects of the inter-governmental agreement(s)
- any MoUs between agencies in different jurisdictions
- any contracts that exist (referred to on p. 41)
- "high-level standards and protocols [governing] the administration, access and use of the DVS" (p. 37)
- "DVS terms and conditions" (p. 42)
- "annual compliance statements" (p. 42)
- "internal and external audits; Privacy and Administrative Reviews" (p. 42)
- "protocol for handling suspected or actual breaches" (p. 42)
- "standards for retention and deletion of personal information" (p. 42)

- "DVS risk assessment and risk management plan" (p. 42)

Of these documents, only three appear to be publicly available – three of the six audit reports from the Privacy Commissioner listed in Appendix 1 (the other three appear to have been 'issued' but not 'published'). The lack of transparency is disturbing. If others of these important documents would be available in response to an FOI Act request (and we can see no obvious reason why they would not be), then the spirit of that Act, as amended in 2010, is that they should be made publicly available pro-actively.

(b) Inadequate and Misleading Disclosure to Individuals

The information provided to individuals is unclear, but it appears to be in many cases inadequate, and, for the reasons explained in section 1 above, may be in many cases seriously misleading.

The PIA Report identifies risks arising (pp. 24, 30-31), but the recommendations in relation to the management of that risk fall far short of the need.

(c) Absence of Public Interest Representation

A considerable governance structure exists (p. 38).

Yet there appears to be no representation whatsoever of the interests of the individuals whose data is the subject of the transactions.

The PIA Report (pp. 21, 29-30) is seriously deficient in that it fails to address the absence of representation of the affected public in the governance structures and processes.

(A minuscule element of the whole is, however, the subject of a recommendation on p. 32).

(d) Encryption

The statements about data encryption are unclear.

In particular:

- is the data encrypted end-to-end, i.e. between the requesting agency and the reference agency, such that the DVS Hub does not see the unencrypted data?
- alternatively, is the data encrypted on each leg, i.e. between the requesting agency and the DVS Hub, and then between the DVS Hub and the reference agency, such that the DVS Hub does see the data in clear?

In either case, which data is encrypted, and which is not?

(e) CertValid

Reference is made to a CertValid service, "which verifies Birth, Marriage and Change of Name Certificates issued by State and Territory Registries" and "is operated at the NSW Registry of Births Deaths and Marriages for all State and Territory Registries" (p. 15).

APF has not previously been aware of this operation.

APF is not aware of any PIA being performed, nor of any consultation with the affected public.

In the case of the Victorian Registrar at least, and in relation to the Commonwealth participation, there is a very strong public expectation, endorsed by the respective Privacy Commissioners, that a PIA be performed.

3. Failure to Manage Function Creep

The PIA Report discusses some of these risks (pp. 27-28), but fails to make any meaningful recommendations.

(a) New Registration Processes

The statement is made that "some new registration processes are being developed" (p. 41), but it is completely unclear what controls such projects are subject to.

It also appears that representatives of the public are being completely excluded from the process whereby these projects are being conducted.

Further, the statement is made that "[these new processes] will not require [the agencies] to collect any additional information from the individuals concerned than would be required of a non-DVS enrolment process" (p. 41). This appears to be an incorrect statement, or at least a statement that is impossible to make without a detailed understanding of the various contexts in which it is envisaged that function creep is intended to occur.

(b) Extension to Medicare

Further, the extension is stated to include "the addition of Medicare card verifications" (p. 15).

There is no evidence of any PIA being conducted, nor any consultation with affected individuals or advocates for their interests. The PIA Report is seriously deficient in that it fails to even discuss this aspect, and makes no specific mention of the desirability of a PIA being conducted.

4. Inadequate Protections for Individuals' Interests

The DVS "is an administratively established program. It does not have governing legislation" (p. 14), and it "operates under the executive approval of the States, Territories and the Commonwealth" (AGD's letter of 14 December 2012).

This creates serious concerns about inadequacies in protection of individuals' interests, because such loose arrangements provide the individual with no rights enforceable in the courts.

The PIA Report is seriously deficient in that the several places in which aspects are discussed lead only to vague and toothless recommendations.

(a) Maintenance of the Data Trail

It is a positive feature of the scheme that (with an important qualification) each of the applying agency, the DVS Hub and the reference agency is provided only with the data relevant to the performance of its function. In particular, (generally) the reference agency does not know from which agency the request came.

However, it can be readily inferred from the text that requests cannot be re-identified, and that no overall picture of the individual's transactions can be produced. Such an inference is incorrect.

The data trail is capable of being re-identified and consolidated, because:

- each requesting agency may retain the requests it issues, identified by its transaction id (VRN1)
- each reference agency may retain the requests it receives, identified by its transaction id (VRN2)

- the DVS Hub retains the cross-reference between VRN1 and VRN2, including the Originating Agency Code (OAC), the Issuer Agency, the document type and the verification response (pp. 14, 46)

In addition, BDM Registrars receive the OAC on all requests.

It is unclear what protections exist to preclude abuse of the data trails by the many agencies involved.

No deletion schedule is specified, implying that all of these agencies may retain the logs for as long as they see fit.

The PIA Report notes that "there is at least the perception of risk of use of the information for new purposes or to track individuals' activities" (p. 22), but fails to make any recommendations in relation to the management of that risk.

(b) Exclusion of the Individual from Agreements

The agreements are all between governments and agencies. None include the individuals whose data is the subject of the transactions. Such obligations and undertakings as arise under the arrangements cannot be enforced by Individuals.

Individuals are at considerable risk from the use of the scheme, in particular:

- a requesting agency may impose considerable burdens on the individual, or may refuse the application for registration, service or benefit, under various circumstances:
  - where a match is not achieved as a result of error by the reference agency (e.g. an error in the database or the matching process)
  - where a match is not achieved as a result of error by the requesting agency (e.g. an error in the compilation of the request, inadequate or unclear instructions to individuals in relation to the data to be provided or keyed)
  - where a match is not achieved as a result of error by the individual (e.g. mis-keying of data into an online form, misunderstanding of the instructions provided)
- nothing in the scheme, nor in data protection laws generally, requires agencies that refuse an application or impose more onerous requirements to provide reasons for doing so (some participating agencies may be under other administrative law obligations to give reasons).

This may result in errors in reference agency databases, and in procedures, instructions and online systems, going undetected for long periods of time, to the detriment of individuals

The PIA Report is seriously deficient in that it fails to identify the lack of power of individuals to enforce any aspect of the arrangements, and its discussion of the risks is inconclusive (pp. 26-27).

(c) Limitations on Private Sector Use

The statement is made that the extension is to "private sector organisations that have a demonstrable legal obligation to identify people" (p. 13).

This is incomplete in two ways. The first is that some instances of legal obligations relate not to identification but to authentication. This appears to be acknowledged elsewhere, e.g. in the third bullet on p. 17. The second aspect is of serious concern. The scope must be declared narrowly and specifically, and must not extend to, for example:

- circumstances other than those that are the subject of explicit legal authority
- identification or authentication by means that are not the subject of explicit legal authorisation. For example, a category of corporation may have authority to seek confirmation against a specific agency, register or database, but not others

The PIA Report (p. 21) is seriously deficient in that it accepts the inappropriate formulation of "demonstrable legal obligation".

It is also of concern that examples are provided (p. 13), but not an exhaustive list of all such legal authorities. Reference is made to "a formal application process", and to approval by the DVS Advisory Board, and to contracts (p. 17). Under current circumstances, there is no mechanism to ensure that the affected public is consulted on this matter, and that the public's interests are reflected in these arrangements.

(d) Agents for Requesting Organisations, not Individuals

The DVS extension proposal relating to agents envisages corporations acting as agents for government agencies, and for corporations, but not for the individuals whose data is contained in the transactions.

This is an unbalanced arrangement, with the result that individuals are at risk of having market power played against them. Such an arrangement also has the effect of excluding individuals from contracts, with the result that they would have no capability to enforce undertakings by other parties.

The PIA Report (p. 21) is seriously deficient in that it fails to identify the lack of power of individuals to enforce any aspect of the arrangements.

Conclusions

The APF's analysis of the DVS Extension Proposal has identified a great many areas of serious concern. A Summary is provided below.

The PIA Report is seriously deficient in that it fails to identify "any 'show stopping' privacy issues, either in terms of compliance with privacy principles for the DVS participants or wider privacy risks or impacts for individuals" (p. 22).

The concerns identified by APF in December 2012 would have been available to AGD in March 2012, had AGD conducted consultations with relevant advocacy organisations for the affected public.

Australian Privacy Foundation

Submission relating to the DVS Extension Proposal

15 February 2013

Summary of Submissions

1. **Descriptions**. It is essential that the descriptions of the DVS and of the DVS Extension Proposal be amended in order to remove the many misleading statements identified above. If not, the Proposal is based on misinformation. See all of s.1 above.
2. **Specific Legislative Authority, Not Consent or 'Consistency ...'**. It is essential that all uses of the DVS be subject to specific legislative authority, and that under no circumstances is use of the DVS justified by spurious claims of 'consent', nor of 'consistency with the purpose for which the information was collected', nor of 'consistency with a demonstrable legal obligation'. See 1(d), 1(f) and 1(g) above.
3. **Communication to Individuals**. It is essential that legislative provisions be enacted that ensure that the nature of DVS is accurately communicated to individuals whose data will or may be used by an applying agency for cross-checking via the DVS with a reference agency. See all of s.1 above, and 2(b).
4. **References to Consent**. It is essential that all reference to consent be removed from communications with individuals, and that the facts be declared, along the lines of 'the provision of this information is a condition of application, and the agency is authorised by law to cross-check its accuracy with the relevant reference agency'. See 1(d) above.
5. **Protections for Individuals**. It is essential that a comprehensive set of protections for individuals be enacted, so that there is no reliance on unenforceable agreements to which the individual is not a party. These must address all aspects discussed in s.4 above.
6. **Governance**. It is essential that the affected public have effective representation on the DVS Advisory Board and the DVS Steering Committee. Because the matters require a considerable degree of understanding of the context and experience of the workings of governments, it is desirable that the representatives be from relevant advocacy organisations, rather than token appointments of individuals. See 2(b) above.
7. **Data-Trail Deletion**. In order to preclude the gradual emergence of an intensive data-trail of each individual's dealings with organisations, it is essential that all data-trails be required by law to be deleted after a short time, of the order of days, not months. See 4(a) above.
8. **DVS Access Extension**. It is essential that extension of access to the DVS by additional agencies or corporations be permitted only in those cases where a formal legal authority exists, and not in other cases involving the same organisation, or against other reference agencies access to which is not the subject of legal authority. See 1(g), 3 and 4(c) above.
9. **Medicare**. It is essential that the proposal for extension to include matching against the Medicare database be the subject of a separate PIA, not only because it represents a new use completely unrelated to the purpose of the data, but also because the database is well-known to be of low quality. See s.3.
10. **CertValid**. It is essential that the extension proposal in respect of CertValid be the subject of a PIA, including public consultation. See 2(d).
11. **Application and Approval**. It is essential that the application and approval process for extensions be formal and transparent processes that include appropriate public representation (as per Submission 6. immediately above), See 4(c).