



**Australian
Privacy
Foundation**

post: GPO Box 1196
Sydney NSW 2001
email: noIDcard@privacy.org.au
web: www.privacy.org.au

13 April 2007

Access Card: Registration

Australian Privacy Foundation's submission in response to Taskforce Discussion Paper No. 3

Contents

About the Australian Privacy Foundation	1
Overall views	2
Inherent conflict in objectives of the scheme	2
Lack of specific detail from the Government	5
Concern about implicit or missing information	5
Matters not considered by the Taskforce	6
Misleading use of notion of 'consent'	7
Data security concerns	7

About the Australian Privacy Foundation

The Australian Privacy Foundation is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about us see www.privacy.org.au

Overall views

As noted in our submission to the Taskforce's Discussion Paper No. 1, the Australian Privacy Foundation (APF) opposes the proposed Access Card, and does not accept that it should proceed.

The APF does not oppose specific balanced proposals to meet important objectives in the areas of social security benefits administration and, separately, health benefits administration. Nor does the APF oppose the use of smartcard technology to achieve those objectives.

However we believe that the Access Card, as currently proposed, is neither the best, nor the least privacy-invasive, means of achieving those objectives.

The Taskforce should recommend a more sensible timetable for the project. We believe that the Government's target of registration commencing in 2008 is completely unrealistic for such a large-scale and multi-faceted technology project. Apart from making a successful and cost-effective implementation more likely, a more realistic timetable would also allow for better consideration of implications for citizens and consumers, and for privacy and other concerns to be addressed.

The specific comments and recommendations in this submission should not be taken to imply acceptance that the proposal should or will proceed. They are made in the event that, despite our opposition, the project does continue.

Inherent conflict in objectives of the scheme

The Discussion Paper highlights the fundamental conflict between the two stated objectives of the Access Card scheme, and between those objectives and the intention of the Government as demonstrated in the way the card (and the underlying system) has actually been designed.

The as-yet unreconciled nature of these conflicts puts the entire rationale for the project at risk, and makes assessment of its impact on privacy extremely difficult.

There are three competing objectives claimed for the Access Card:

- improving access to health and welfare payments
- tackling welfare fraud, and
- offering consumers (and third parties) the 'convenience' of an all-purpose proof-of-identity card.

The Discussion Paper notes that:

"Throughout the development of the entire Access Card proposal there has been some tension between pressures to require a "gold standard" form of proof of identification ... and a standard more directly related to and appropriate for the facilitation of welfare payments" (p.19).

This Discussion Paper takes the view that the purpose of the Access Card scheme is “to facilitate health and welfare payments, not to establish identity as such” (Discussion Paper # 3, p.18).

However the Discussion Paper later contradicts this view, when describing the purpose of the registration aspect of the system. Rather than being intended to enrol people as efficiently and fairly as possible, so as to enhance their ability to access payments, the “stated aims” of registration for the card are described as “that (the registration system) will be capable of detecting false matches ... and that the system will not be open to abuse or improper use or access” (p.43).

Furthermore, the Taskforce has previously said that the “reduction or elimination” of losses caused by fraud (whether provider fraud or recipient fraud)“ is a key driver for the implementation of the access card” (Discussion Paper # 1, p.29).

Indeed the only quantified benefits in the ‘business case’ prepared for the Government relate to projected savings by reducing welfare fraud, and KPMG recommended that the system be made compulsory, because it would not otherwise create a “sound value proposition” for the Government (Department of Human Services, *Health and Social Services Smart Card Initiative*, Volume 1: Business Case, KPMG, February 2006, *Public Extract* released June 2006, p.10).

We submit that the three claimed objectives of the Access Card system cannot be reconciled, and that discussions around the appropriate means by which to register people have only served to highlight this fundamental problem with the proposal.

The problem lies in the fact that the Government’s costings and justification for the project appear to rest on the project being designed to suit one objective (reduction of welfare fraud), yet any leeway offered towards meeting either or both of the other two objectives means that those costings will be wrong.

We submit that the true net ‘value’ of the Access Card project – its costs, risks, tradeoffs and benefits – cannot be calculated until these competing objectives have been resolved. As a society, we cannot say whether or not the privacy risks inherent in the project are ‘worth it’, until we know what the benefits will be.

The more that the registration system’s hurdles are lessened to reflect the first objective (improving access to health and welfare payments), the more that the claims about the scheme achieving \$1.6 to \$3 billion in savings (from reduced welfare fraud) must be put in doubt.

For example, either the system will facilitate access to services (which suggests low POI threshold requirements for those wishing to register), or it is intended to establish a high-value unique identifier for every Australian, to minimise identity-based fraud (which suggests high POI requirements). One of these objectives must lose out.

In particular, if the Government were to accept your preliminary recommendation that only one foundation document is needed to “commence identity for registration purposes”, and that the one document could be a birth certificate (p.17), then all the claims by KPMG about the savings to be generated will be worthless.

The Government has already argued that birth certificates alone are weak forms of POI – they have quoted some study by Westpac which suggests that a quite high percentage of ‘birth certificates’ are fake. This situation will be exacerbated now that we know that the proposed Document Verification Service will not be available to offer verification of birth certificates (unlike passports) until at least 2010.

Furthermore, the example consistently used by Government ministers and the Office of the Access Card to illustrate why (they claim) the Access Card is needed – the example of the woman who registered the birth of 9 sets of fake twins and used those genuine birth certificates to claim welfare benefits from Centrelink – only serves to demonstrate how easy it is to fool the system if only birth certificates are relied upon. (We recently pointed out to the Chief Technology Officer, Marie Johnson, that the proposed registration system for the Access Card would *not* prevent this scenario occurring again; she had no rebuttal for us.)

Likewise if “known customer” rules for Centrelink and DVA clients are accepted by the Government as acceptable POI for registration purposes (as proposed in the Discussion Paper at p.23), how will this address the claims of existing identity-based welfare fraud that are alleged to be ‘solved’ by the Access Card?

Either there is an existing problem of fake identities being used in Centrelink, DVA and Medicare which needs to be sorted out through rigorous new POI (which your Taskforce clearly does not like on the basis that it will lead to service denial for the disadvantaged and wrongly accused), or there is no fake-identities problem (in which case the Government is misleading the public about the problem), or there is a problem but it won’t be fixed because of the project’s competing objectives (in which case the Government is misleading the public about the solution).

Other practical difficulties with registration mentioned in the Discussion Paper include the problem of people who object to having their photograph taken (see pp.27-28, 42). Again, while we admire the Taskforce’s thinking about how to ensure that such people are not denied health and welfare payments, how can the Government’s claims about reducing identity-based welfare fraud be borne out if you allow exceptions to the registration rules? We submit that if the system is robust enough to withstand exempting some people from having their photograph taken on religious grounds, then why not exempt everyone who doesn’t want their photograph included? We argue that the photograph should be scrapped entirely, or at the most included as a voluntary feature.

A similar problem is highlighted by the discussion at pp.19-20 of ‘interim’ versus ‘full’ registration. If, as the Taskforce proposes, no benefits can be denied a person with only ‘interim’ registration, what is the practical difference between the two statuses?

Does this suggest that a card with ‘full’ registration status will be useful as an all-purpose ID card suitable for third party use, but an ‘interim’ one is not? If there is to be no visible indicator of ‘interim’ versus ‘full’ status on the surface of the card, and third-party access to information on the chip (other than concession status) is to be prohibited (Chief Technology Architect Marie Johnson quoted, in “Banks shut out of smartcard details”, Australian Financial Review, 10 April 2007, p.49), how is the different status to be communicated to anyone?

Either there should be no such distinction between ‘interim’ and ‘full’ status, or the existence of such a distinction will both demonstrate that the Access Card is indeed designed as an ID card, and the proposal will reduce already disadvantaged people to second-class citizen status.

Lack of specific detail from the Government

Too many details about the registration system have still not been worked out by the Government. This Discussion Paper doesn't answer enough of the questions about registration outstanding since our submission to Discussion Paper # 1 almost 12 months ago, which means we can't make meaningful comment on what the privacy issues will be.

For example:

- p.12 – the Taskforce hasn't dealt with **concession status** at all
- p.16 – there is no explanation of what the **Emergency Payments Number** is, or how it will work
- p.17 – there is *still* no decision on what **foundation documents** will be required for registration – not even a draft list
- p.24 – we *still* don't know what the **chip size** will be
- p.24 – we still don't know **whether 'optional' data will be stored on the Register**
- p.32 – strategies for **managing the flow of registrations** are yet to be developed
- p.41 – the Taskforce cannot yet address the **adequacy of biometric photos or the data security** that will apply to them
- p.48 – the Taskforce has a list of outstanding questions about **replacement cards**

It is meaningless to leave these many and varied issues entirely up in the air, and pretend that Australians have been 'consulted' about the registration processes for the Access Card.

We submit that the Taskforce should seek answers to the outstanding issues, and when answers have been obtained, conduct a further round of consultation. There is no valid reason for the Government to rush this project ahead without these details being fully considered.

Concern about implicit or missing information

We also hold concerns about what is not explicit about the project based on Government materials to date, but which is implicit in the Taskforce's thinking, as represented in Discussion Paper # 3.

For example:

- p.8 says "other available technologies" may be used to register people with difficulties – does this mean other types of biometrics are being considered?
- p.9 refers to census and electoral roll procedures used to contact households, and p.34 refers to AEC offices and local councils as possible registration venues because they already have data on people too – does this mean there is a proposal for some collaboration / data-sharing with (or data-collection from) councils, the AEC or ABS?
- p.12 refers to people needing to 'consent' to the sharing of their data between agencies – what new data-sharing is envisaged? The Government has previously said 'none'.

- p.16 refers to the possibility of additional data being needed beyond that already specified in the Bill – what new data is envisaged?
- pp.23-27, in the section headed “additional information to be recorded in the access card system”, details medical data, organ donor status, emergency contact numbers, and other uses – it is not clear how any of this is about “Registration” (the topic of this Discussion Paper # 3), unless these additional uses of the *card* are intended to also be recorded on the *Register* – will this information be recorded on the Register?
- p.27 – the Taskforce suggests victims of domestic violence may be a special category of people who require exemptions from the normal rules for registration – why? The other categories identified (people with particular religious concerns manifest in their facial hair or dress, people with disabilities, the infirm, indigenous communities and the homeless) are because either they cannot easily produce the right POI, or because they have an objection to being photographed a certain way – but why victims of domestic violence? Presumably you have identified victims of domestic violence because they have something very specific to fear from having their details on the Register (as we have always said they would) – but that point needs separate exploration, as it suggests the Taskforce does not have faith in the data security arrangements for the Register itself, as opposed to there being some problem with the act of registration (POI, attending an office, or being photographed)
- p.42 – refers to dangers of “compulsorily photograph(ing)” people with psychiatric problems, yet the system is supposed to be “voluntary” (the Government’s claim) and conducted “with informed consent” (your words, p.12) – does this suggest some new element of compulsion?
- p.51 – says that the Discussion Paper has (prior to that point) identified a number of issues on which it seeks public input, and mentions “the voluntary inclusion of an identification of Aboriginality”. This is the first point in the Discussion Paper that we can see that this issue is raised at all, and without any discussion at all - does this suggest the intention to introduce some new element of data about ethnicity which has been previously denied by the Government?

Matters not considered by the Taskforce

The Discussion Paper does not mention the registration process for children, who will be listed on the Register, but not issued cards. We submit that this is an unfortunate oversight, and that the impact on the 4 million children (and their parents) should be considered with further rounds of consultation.

For example the discussion on p.18 of the secondary identity documents needed for POI fails to recognise that the vast majority of children will not have any of these documents (drivers’ licences, student cards, firearm licences, etc).

How will registration work for children? As noted above, if only birth certificates are accepted, a major weakness will be introduced into the scheme, and the very example used by the Government to justify this whole project – the woman who registered 18 non-existent children using genuine birth certificates – will be able to be perpetrated again. This casts doubt over all the Government’s claims about how the system will prevent identity-based welfare fraud from occurring.

The Discussion Paper also does not mention how information about family relationships will be proven, or how entries on the Register of related people will be

linked together. We cannot make comment on the privacy impacts of the scheme without knowing any detail about how it might work.

Misleading use of notion of ‘consent’

We submit that the Taskforce has misused, or misunderstands, the term ‘consent’.

For example, at p.12 the Discussion Paper appears to confuse the purpose of a standard privacy notice (as required by IPP 2) with ‘informed consent’. Privacy notices offer a one-way communication of information only. They do not seek a response from the person. They do not suggest the person has any choice in the matter – they are simply being informed. By contrast, the process of seeking ‘consent’ requires a response (either consent or refusal of consent), and a means by which the agency concerned can deal with people who respond in the negative.

Further, the Discussion Paper suggests at p.8 that people will need to ‘consent’ to the flagging of any of their relationships with government agencies. On what basis is consent needed? How could the Access Card system work if the card-holder said no? Surely without their relationship with the various agencies being flagged, they would not get their benefits paid – in which case, why would they enrol in the first place. We see no evidence that ‘consent’ will affect this aspect of the scheme.

Likewise p.12 also refers to people needing to ‘consent’ to the sharing of their data between agencies. We disagree. This statement ignores the many existing exemptions to the Disclosure principle under the Privacy Act 1988 which do not rely on ‘consent’, and also ignores the many examples of other legislation which allow law enforcement agencies, the Tax Office, ASIO and the like to obtain people’s personal information without their consent (and in some cases, without their knowledge either).

We argue that the Taskforce should clarify its comments on ‘consent’ as a matter of urgency; to fail to clarify these statements will result in misleading responses during the public consultation process.

We argue that the Taskforce, by inappropriately using the word ‘consent’, is misleading the Australian public into believing there is more privacy protection for their personal information than there is in truth. This false sense of security will affect the validity of the entire public consultation process unless it is rectified.

Data security concerns

We have a number of concerns about the data security aspects of the registration system, as they are described in the Discussion Paper.

For example:

- We strongly believe that sending out cards by ordinary mail, even if PIN protected (proposed at p.8), is ludicrous. Ordinary mail is highly prone to theft. The Access Card is an identity document that can be abused, even if some of the data on the chip is PIN protected. The costs and risks of identity theft should not be shifted by the Government onto individuals, and so we argue that cards should be sent out by registered mail only.

It should be noted that when DFAT switched from using registered mail to ordinary mail, presumably in order to save money, the number of stolen

passports rose dramatically, and the Government was forced to return to using registered mail. The difference was remarkable: when using ordinary mail in 2001-02, on average 162 passports were reported as lost or stolen “in the mail” each month; this figure dropped to 21 per month as soon as registered mail was reintroduced in 2002-03 (see DFAT Annual Report 2002–03).

- We strongly reject the proposal to include the existing Medicare number in the Register (see p.17). That this idea was even proposed by Medicare Australia shows a complete disregard for either the technical benefits or the privacy safeguards of having a smartcard and register system in the first place.

Furthermore, it is evidence of yet another example of pushes for function creep from the agencies in control of the project.

- We strongly agree with the Taskforce’s view of the need to delete or destroy the copies of POI documents once they have been checked at registration (see p.21). However we go further to argue that copies of POI documents should not be scanned or copied or stored in the first place!

As we have argued before, the registration system should not commence until the Document Verification Service is fully operational, which would allow instant, online verification of the four primary Australian-issued POI documents (birth certificates, drivers’ licences, passports and citizenship certificates).

We suggest that funding should be provided to the States and Territories to get their birth certificates into a state where real-time, online verification can occur; this would be a more useful way to spend the Access Card budget than developing an inefficient registration process reliant on manual checking of paper systems.

For those with only POI documents issued overseas, other fast verification options should be explored, to avoid the scanning or storing of such documents, in order to minimise the risk of identity theft for this significant number of Australians.