



GPO Box 5057
Melbourne Victoria 3001
Australia
DX 210643 Melbourne
Level 11
10-16 Queen Street
Melbourne Victoria 3000
Australia
Telephone 1300 666 444
Facsimile 1300 666 445
www.privacy.vic.gov.au
enquiries@privacy.vic.gov.au

27 July 2006

Professor Allan Fels AO
Chair
Access Card Consumer and Privacy Taskforce
PO Box 3959
MANUKA ACT 2603

Dear Professor Fels,

**The Australian Government Health and Social Services Access Card (the Card) –
Access Card Consumer and Privacy Taskforce (the Taskforce) –
Discussion Paper No. 1**

The following comments on the Taskforce's first Discussion Paper address only the main privacy issues. Office of the Victorian Privacy Commissioner (OVPC) assumes that a primary data protection test, necessity, has been or will be met.

1.0 Legislative authority

- 1.1 The discussion paper raises (page 21) the key issue of legislative authority. This is of critical importance. There should be specific legislative authority for the Card, as there is for the use of the Tax File Number. Legislation should establish clarity of purpose. If the primary purpose is established, other privacy protections will follow, such as the clear formulation of related secondary purposes.
- 1.2 Safeguards, such as sanctions for misuse, are best made statutory and enforceable. A purpose-built statute would make the scheme subject to Parliamentary scrutiny, both by committees and, when amendment is sought by Government, by Parliament as a whole. This is important because of the likelihood that over time the scope of the scheme will widen ('function creep'). Function creep seems inevitable for a scheme that is likely over time to underpin most of the population's dealings with all governments in Australia.

2.0 Existing privacy protection

- 2.1 The discussion paper (page 27) refers to a number of Commonwealth statutes which provide for privacy protection and states that the Access Card will operate in ways entirely subject to the requirements of these legislative provisions. It makes specific reference to the *Information Privacy Principles* (IPPs). The federal IPPs are over 18 years old and out of date. There is inconsistency between those IPPs and

other state legislation such as the Victorian *Information Privacy Act*. The federal Act is the subject of a current inquiry by the Australian Law Reform Commission. If the Card is to serve present and future needs, it should not be assumed that the safeguards of the past will do. It may be that a more stringent privacy regime than the one provided by the present Commonwealth *Privacy Act* is required.

3.0 Enrolment

- 3.1 There are a number of privacy issues that arise from what may be termed *enrolment* for an Access Card.
- 3.2 The discussion paper refers to applicants for a Card having to provide "proof of their identity". "Proof of identity" is a phrase that has become common parlance in much public sector documentation. The term implies an illusory certainty and is best avoided. The Taskforce will assist debate if it declares that there is a difference between the oft-used term "proof of identity" and the more appropriate term "evidence of identity". People are rarely able to *prove* their identity, but they are able to provide *sufficient evidence* that they are who they claim to be.
- 3.3 A core issue is how the scheme would enrol large families and people with multiple roles. If it is proposed to have a photograph on the Card:
- Is it intended that this will be a photograph of each member of the family or just a representative (e.g. a parent of a child)?
 - What arrangements will be made for situations such as adult children holding a power of attorney for parents who need to access services? Will the Card contain a photograph of the holder of the power of attorney, or the person who is being provided with the service, or both?
 - How will other care arrangements such as foster children and guardianship be dealt with?
- 3.4 The problems referred to in 2 above raise the question as to whether a photograph on the face of the Card is practical or desirable. It is noted that the image will be contained in the chip. A photograph on the face of the Card inevitably leads to people being required to produce the Card as photo identity for purposes other than the purpose for which the Card was issued. In spite of the statement that it is not a compulsory ID Card, it becomes one *de facto*. In addition, there is a question of human dignity. Enrolment presumably involves having one's photo taken. Leave to one side the similarity with being "processed" by police for a mugshot. Some people, such as those who cannot look after themselves through old age or infirmity, or those who are severely disfigured, may find the enrolment process - as well as the photo and requests to produce it - a discomfort disproportionate to the benefit obtained. So might their carers.
- 3.5 The discussion paper refers to the recording of "digital signatures" of Card holders. Clarification is sought as this could be interpreted in three ways, with each having markedly different implications for the system to be developed:
- The simplest is merely an image of a handwritten signature, which is current practice for the vast majority of government issued Cards. Human interpretation of a match between stored images and a freshly presented signature is a hit and miss affair, so it does not afford a secure option.
 - More complex is a digitised signature, rendered in digital form, as proposed for the Card photo. This could result in a person losing access to benefits if there is not a sufficient match. Many persons' signatures vary significantly on different occasions when they write them. This may be a poor safeguard.

- Computer generated digital signatures are not sourced from handwriting. Sometimes referred to as PKI (public key infrastructure), they involve the encryption of messages using certified public and private 'keys'. The issues surrounding handwriting consistency do not arise, but PKI would significantly increase the technological complexity, and costs, of the Cards and related database.

3.6 The discussion paper does not address the issue of if, or when, government may decide to withdraw a Card. Will it be withdrawn or suspended, for example, if a person is imprisoned, or incapable through mental illness of looking after their own affairs, or because they have failed to meet certain administrative requirements? The more accepted the Card as a token of identity, the more invisible becomes the person without one. The implications of withdrawal or suspension of a government-issued Card will doubtless emerge in greater detail as the Taskforce continues its work. OVPC encourages further careful scrutiny of this issue.

3.7 The Card will have the Card holder's number (page 11). It is stated that the number will be the consumer's current Medicare number "reformatted to bring it in line with international standards". It is not clear what is meant by that statement. A number allocated to each Card holder will become a unique identifier for the Card holder. National and international data protection standards constrain the assignment and use of unique identifiers. If it is administratively necessary to assign a unique identifier then the requirement to disclose to, and the use by, other organisations for purposes unrelated to the purpose of initial assignment of the number needs to be expressed and controlled by legislation in the same way as the Tax File Number.

4.0 Purpose of collection

4.1 Data protection standards, nationally and internationally, require that personal information should only be used for the purpose for which it was collected, related secondary purposes, with consent, or other specified purposes. People should be given notice of usual uses at the time of collection or as soon as practicable afterwards. The fact that a lot of the data that needs to lie behind this Card scheme was collected, often compulsorily, for purposes unrelated to the present proposal needs to be addressed.

4.2 The Taskforce flags the issue of function creep (page 22). This will inevitably happen if a government-issued Card is in the hands of an estimated 16 million Australians and it is believed they were reliably enrolled for it. State and territory governments, law enforcement authorities and the private sector will find multiple uses for the Card and/or its unique identifier. If it is intended to win public acceptance of the purposes and legitimacy of the Card, it is necessary to plan openly for function creep, not all of which is *a priori* bad. The process that produces function creep needs to be open, legitimate and reviewable. Parliament should do it, and have the capacity to tailor any new safeguards necessary to the particular function envisaged.

5.0 Data Quality

5.1 Data quality is a key information privacy principle. Poor quality data can have significant adverse effects on persons, especially if the wrong information leads them to lose benefits to which they are entitled, or to be wrongfully accused and shunned.

- 5.2 The paper states (page 19) that all of the data to be contained on or in the access Card itself, or in the Secure Customer Registration Service (SCRS), is contained on existing files and records of participating agencies. The exceptions are photograph and signature. Using existing databases is fraught with problems. The quality of existing data held on existing databases is uneven, and it would be a brave step to assume any of them sufficiently reliable. To attempt to match and produce a single identity database from such a data matching exercise is likely to produce even poorer quality. There is a multiplier effect in utilising unreliable data for other purposes.
- 5.3 It is proposed that a person will be able to change their personal details with one agency and those details will be changed with all other agencies interacting with the individual, via the SCRS. If a person uses multiple agencies the database linkage required to accurately achieve this is significant. The Taskforce is encouraged to test the details with the scheme's architects and explain more.

6.0 Data Security

- 6.1 The paper highlights a number of concerns about data security, as follows.
- 6.2 The proposal will result in a massive database containing personal information about most Australians. The bigger and richer the database, the more attractive it is for those who want to mine it, for those who are prepared to sell it, and for mistakes through human error to replicate. OVPC has considerable experience with the problems of ensuring the security of the Victoria Police database. A significant literature on these issues exists internationally. Organised crime will anticipate the implementation of the system and make every effort to penetrate the security layers. This requires robust security which goes beyond existing protections. Public confidence can reasonably be withheld, pending much better explanation of how the database will be secured.
- 6.3 The paper acknowledges identity theft and the problems it causes to people. Identity theft is one of the worst invasions of privacy. If individuals have only one Card as a means of accessing multiple government services, more "identity eggs" are in one "basket".
- 6.4 It is stated that the Government believes that having data on both sides of the Card will make it "much more difficult for unauthorised people to collect this data in one simple operation." How much more difficult? For instance, driver's licences may nowadays be photocopied preparatory to being misused. It is not difficult to request a Card, go to a back office and make copies of each side of a Card. Unless OVPC has misunderstood, this is clearly not a significant data security measure.
- 6.5 It is proposed that individuals will be able to access and correct their own data. Creating a system that allows individuals to electronically access and update data adds significantly to data security and data quality problems. Home computers are a major source for the spread of malevolent software.
- 6.6 The development of an access control regime for the SCRS will be a major exercise. While it is obvious that only 'authorised persons' will be permitted access, the use of this term understates the enormity of the task that lies ahead to ensure that not only the right people have access, but that their access permissions are

suitable to their working context. Not only will this system be accessed by a multiplicity of public and private sector organisations, but as yet loosely defined hardware is involved (e.g. card readers). Granularity of access is rarely done well, yet it is a key feature of the proposed system. The Taskforce is urged to make this area another focus.

- 6.7 Card replacement will be a critical data security issue. Replacing lost Cards by mail is recklessly insecure. If replacing a lost Card requires a personal attendance, it will be important to remember the people who need help to attend, and need continuity of services while they wait for the new Card.
- 6.8 One of the proposed benefits is easier access to benefits in an emergency (e.g. natural disaster). Some emergency situations are likely to be the very time when Cards are lost or destroyed (unless they are carried at all times by all people). More broadly, this goes to proportionality: how often is the average Australian involved in a natural disaster or other emergency?

7.0 Conclusion

- 7.1 A central test in assessing any proposal from a data protection perspective is proportionality. In the context of this Card proposal, the Taskforce is urged to focus on the issue of whether the benefits in revenue collection and revenue protection (i.e. responding to Medicare or other benefits fraud) are proportionate to the costs of the Card to the majority of Australians, in dollars, time and increased government powers.
- 7.2 Many matters of detail need to be addressed. When the proposed Access Card was formally announced I published a Smartcard Privacy Checklist as a contribution to the debate. I attach a copy of the checklist. I believe that if its 20 questions are answered satisfactorily, the Taskforce will have gone a long way to satisfying itself that the legitimate privacy concerns associated with the Card scheme have been addressed.

Yours sincerely,



PAUL CHADWICK
Privacy Commissioner

Enc. Smartcard Privacy Checklist

Smartcard Privacy Checklist

20 questions for the public to ask persistently
and for governments to answer satisfactorily
about a government-issued smartcard
that most Australians would need to have

The information

- 1 What information about me will be on my card?
 - what will be visible on the card?
 - what will be on the microchip?
- 2 What information about me will be on the supporting databases or linked to them?
- 3 What information will be compulsorily on the card and databases?
- 4 What information will be there only if I choose?
- 5 Who will decide what other information will be gradually added over time -
 - me, by choice?
 - Parliament, by passing specific legislation each time?
 - Ministers/public servants, by using general powers?

The purposes

- 6 Who will have access to the information about me on my card or in the databases?
 - which parts of government?
 - which businesses?
- 7 What will they be allowed to do with my information?
 - eg will the photo collection be made available to police or any other authorities?
 - eg any medical research, taxation or border control activities?
- 8 What will they be prohibited from doing?
 - eg demand my card before I can vote?
 - eg link my data to the data about my relatives or associates?
 - eg connect the smartcard scheme with Census data in any way?
- 9 Will the unique number on my card be allowed to be used to match my information with other information about me held by the federal government, state/territory/local government, or private organisations?
- 10 If so, by whom and for what purposes?

The safeguards

- 11 How will they know that the information they already hold about me is accurate to start with?
- 12 How will they keep information about me accurate?
- 13 How will they keep information about me secure?
- 14 Will I have the right to see and correct my information?
- 15 If something goes wrong and my personal information is at risk, will I be notified so that I can take steps to protect myself?
- 16 If my card is lost or stolen, how will I still be able to deal with government while the card is being replaced?
- 17 On what grounds could they withdraw or cancel my card against my will?
- 18 Who will independently oversee the smartcard scheme?
- 19 What powers and resources will the oversight body have and how can Parliament ensure its independence?
- 20 How often will the smartcard scheme and the oversight body be periodically and openly reviewed by Parliament to help ensure that I can trust government to collect and handle my personal information according to adequate standards?



Office of the
Victorian Privacy
Commissioner

www.privacy.vic.gov.au