



**Australian
Privacy
Foundation**

GPO Box 1196
Sydney NSW 2001

www.privacy.org.au

30 March 2007

Senator Chris Ellison
Minister for Human Services
VIA EMAIL

Re: the Access Card – a way forward

Dear Minister,

I am writing with respect to the Access Card project to suggest some ideas for ways to achieve the project's objectives, while also resolving many of the problems recently identified through the Senate Committee's inquiry. We hope that an opportunity might arise to candidly discuss with you some of these ideas.

Project objectives

As we understand it, the Access Card project's objectives are two-fold:

- streamline or improve access to government services, and
- minimise the chances for fraud in the welfare and health benefits systems.

We support these objectives. We also support the appropriate use of smartcard technology to achieve those objectives, and the Government's stated intention to avoid the creation of a national ID card system.

However we do not believe the Access Card project, as currently proposed, presents the best way to achieve those objectives. The design of the Access Card project has been allowed to expand beyond what is necessary to achieve those objectives, incorporating unrelated and third-party objectives. Unrealistic timeframes and a bolt-it-on-later approach to privacy management have also contributed to this project's fundamental difficulties.

We suggest that a back-to-basics rethink of the project is needed to ensure that the Government's two fundamental project objectives can be achieved in the most cost-effective, risk-averse and least privacy-invasive manner. The government should not require, facilitate or encourage, use of the cards for anything other than the two objectives.

Project concerns in brief

The collapsing of Medicare and other cards together

The Medicare card, as it exists now, is a universally-held card of limited applications. The only time one uses a Medicare card is when paying for, or seeking a refund of payment for, health services.

By contrast the other 16 Centrelink and DVA cards are held by smaller numbers of people, but used in a much wider range of applications – both for direct government service provision, payments and rebates, and when claiming concessions from an unlimited range of third parties, from bus ticket sellers to cinemas.

Many of the privacy concerns with the Access Card project stem from the rolling together of the Medicare card with the other 16 cards, such that the result is a universally-held card of limitless applications. When a photo, signature and card number are added to the surface of the card, it becomes a national ID card, plain and simple.

We suggest a re-think of the need to roll together Medicare cards with the other 16 welfare benefit cards. Separation into two projects would be a terrific step in the right direction.

The underlying database

The Access Card project is predicated on there being one card, and one registration per person, in a whole new database.

However this misses the great benefit of smartcard technology. Smartcards can actually handle multiple 'customer numbers' and customer identities in a secure fashion. A whole new database is simply not needed to gain the benefits of this technology.

The single number / single database aspect of the project raises significant privacy, data security and identity theft risks. Again, we suggest a re-think of this aspect of the project.

The use of biometric photos

We believe that the claims made for the benefits of biometric photos and facial recognition technology simply do not stack up when we are talking about one-to-many matching across a database of 16 million people. Even with a false positive error rate as low as 1%, a photograph of Cornelia Rau taken in immigration custody – or your photograph when you go to enrol in the system for the first time - would generate 160,000 "matches".

The notion that this technology will prevent duplicate enrolments in the system, or will substantially assist Immigration, ASIO or Police to identify individuals, is technically unrealistic. Furthermore the costs and risks of this 'bleeding edge' technology are excessive.

The biometric photo / facial recognition aspect of the project raises significant privacy, data security and identity theft risks. This is particularly so when the biometric templates for the entire population will be held on a central register, rather than just stored in the card's chip

for authentication purposes. Again, we suggest a re-think of this aspect of the project. Standard digital photographs are perfectly suitable for fraud control purposes.

Some ideas for a way forward

In order to reduce the likelihood of the Access Card working as a national ID card, we suggest that the following ideas deserve consideration.

Fundamental principles

- We first suggest that you separate out the project into two projects: the first being just an upgrade of the Medicare card, and the second being to deal with the other 16 Centrelink and DVA cards.
- We suggest that all design features, scope and functionality that do not relate to the project's two objectives be immediately dropped. This includes the voluntary medical information and other 'optional' features; and precludes designing the system to suit the identification requirements of banks. Both personal information security and program cost effectiveness would be advanced by the adoption of straightforward and effective legal, administrative and technical means to permanently limit the features, scope and functionality of the card system.
- We suggest that the use of biometric photographs be dropped.
- Card numbers should be unrelated to customer numbers, and no new single 'person' number is needed.
- To maximise the fraud control benefits, and in line with the National Identity Security Strategy, we suggest that neither project commence until the Document Verification Service is successfully operational.

Suggested Medicare card model

- upgrade the Medicare card from magnetic stripe to smartcard technology
- ideally, maintain the Medicare card as a family card, not an individual card
- have *either* the card-holder's name(s) or photo(s) on the surface of the card – but not both:
 - 'name only' model: make the photo readable from the chip, but only for authorised people (relevant Medicare Australia staff, and health service professionals providing a Medicare-related benefit), or
 - 'photo only' model: make the name readable from the chip, but only for authorised people (as above)
- all other customer information, including card number and customer number, to be stored on the chip
- store current Medicare / PBS safety net status information on the card's chip
- legislate to only allow people to ask to see or check the card (or the card's chip) where the person is seeking a Medicare benefit
- rollout new cards according to the existing seven-year replacement timetable

Both the 'name only' model and the 'photo only' model allow people to access Medicare-related services, without the card being in any way useful to unrelated third parties as an 'ID card'.

The 'name only' model means that the service provider can be satisfied that the carrier is entitled to the Medicare service requested, so long as either (i) the person presenting the card can show other evidence of being the person with that legal name, or (ii) the service provider can use a photo-readable card reader to view the photo from the chip, and visually match the photo to the person in front of them.

The 'photo only' model means that so long as the person presenting the card visually matches the photo on that card, the service provider can be satisfied that the carrier is entitled to the Medicare service requested.

From a privacy point of view, the 'name only' model is preferred. While we understand that the cost of providing photo-readable card readers to all health service providers may be excessive, we would believe that a slower rollout will help keep costs down as the cost of this technology falls.

Suggested combined Centrelink / DVA card model

- combine the 16 existing cards into one "welfare benefits and concession" card
- use smartcard technology
- use existing Centrelink and DVA customer databases, rather than build a new Register
- for people with permanent concession status: print concession status on the surface of the card
- for people with changeable concession status: store current concession status information on the card's chip
- have *either* the card-holder's name or photo on the surface of the card – but not both (as above – see discussion re Medicare card)
- all other entitlement and customer information, including card number and customer number(s), to be stored on the chip instead
- legislate to only allow non-Centrelink/DVA people to ask to see or check the card (including the card's chip) where the person is seeking a concession benefit or discount

If you would like to discuss these matters in more detail please do not hesitate to contact me on (02) 9432 0320 or 0400 432 241.

Yours sincerely

Anna Johnston
No ID Card Campaign Director,
Australian Privacy Foundation