Australian
Privacy
Foundation

p o s t: GPO Box 1196
Sydney NSW 2001

e m a i l: enquiries@privacy.org.au

w e b : www.privacy.org.au

31 July 2006

The 'Access Card' proposal

Australian Privacy Foundation's submission in response to Taskforce Discussion Paper No. 1

Executive Summary

No matter how the Government describes it, the proposed 'Access Card' is a national identity card. It poses as many, if not more, risks to privacy as did the 'Australia Card' proposal of 20 years ago. Most of the population would be required to register for and hold a card if only as proof that they are eligible for Medicare benefits – a near universal entitlement.

The Government's assertion that the proposal does not amount to a national identity card scheme does not stand up to scrutiny. Public debate about the proposal needs to be based on the reality rather than government 'spin'. The Taskforce should form and publicly state its own view on this important issue.

No matter what assurances are given about how the so-called 'Access Card' will be used, it will inevitably become mandatory in effect for an increasing number of transactions in both the public and private sectors. Apart from the declared uses for benefit claims, it is inconceivable that the card would not become primary evidence of identity for such transactions as electoral enrolment and voting, opening bank and other accounts, posting parcels and opening a mobile phone account, and to establish eligibility for a range of state and local government, and private sector concessions.

No matter what security systems are promised, the creation of a national identity database will inevitably lead to an increase in the unauthorised access to and use of personal information. Governments have been unable to prevent the misuse of data on their existing databases, and the risks arising from the creation of a national database are far greater.

The APF opposes the proposal 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. The threat to privacy from a combined initiative is, and will always remain, too great for it to be acceptable.

Clearly, there is a need for informed and mature public debate about the proposal yet the Government has not provided sufficient information to allow this to occur.

The Taskforce should recommend publication of the full KPMG Business case, the contemporaneous privacy advice and further details of the proposal as soon as it becomes available.

The public cannot make judgements about whether any loss of privacy is acceptable without being able to weigh that loss against objective measures of the benefits. The Taskforce should not confine itself to analysis of the privacy and other implications for citizens and consumers of government services. The Taskforce should also insist on the quantification and independent validation of alleged benefits and also the public presentation of what less privacy intrusive alternative means of delivering those benefits have been considered.

The Taskforce should publish all submissions that it receives, unless there are claims of confidentiality. Any such claims from public sector agencies and industry bodies must be justified. The Taskforce should publish its findings, recommendations and reports to aid continued public debate.

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.

The Taskforce should recommend a more sensible timetable for the project. We believe that the Government's target of card issuance 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 Taskforce should closely scrutinise the extent to which the proposed card and underlying systems including the Secure Customer Registration Service might actually contribute to, rather than alleviate the threats of, identity fraud and theft. The Taskforce should enquire into the many expert views, including from some of the Government's own advisers, that placing too much emphasis on centralised systems may increase rather than reduce vulnerability.

The Taskforce should question the need for the various proposed features of the card, the SCRS and associated systems and processes, in particular the need for the name, photo and unique number to be displayed either on the card faces, the card chip and/or the underlying databases. Superficially minor differences in the combination of these elements will result in large differences in the privacy implications.

The Taskforce should critically assess any claims about data quality and data security in light of the experience of previous technology projects, and in light of the inevitability of human error and of some level of unauthorised use and disclosure. No systems can be guaranteed 100% secure and accurate, and the public is entitled to know what the consequences of the inevitable security breaches and quality failures might be.

If the access card proposal goes ahead (which the APF believes should not occur), it is essential that it be governed by specific legislation which sets the parameters for use of the card and number, the purpose and scope of the SCRS, and access to the underlying information. It will not be sufficient to rely on existing secrecy provisions and the Privacy Act, which between them allow for a much wider range of secondary uses than will be publicly acceptable for the access card data. The Taskforce should recommend legislation, and a governance framework, that provides the maximum protection against future function creep.

CONTENTS

Executive Summary....1
About the Australian Privacy Foundation....3
The consultation process....4
Not enough detail....4
Not enough transparency....4
Not enough time....5
Privacy concerns treated in tokenistic way....5
A hamstrung Taskforce....6
The project's rationale, claims and scope....7
The Taskforce must review claims about benefits....7
The Access Card – trying to be all things to all people....8
Identity issues....10
A national ID card....10
A national ID number....10
Impact of the proposal on identity fraud....11
Alternative models - what should be considered....13
It's not just about the ID card - other privacy and data security concerns....14
International experience....15

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

The consultation process

At the outset we wish to note our disappointment in the Government's consultation processes on the so-called Access Card proposal.

Not enough detail

Beyond broad statements and platitudes, the Government has revealed scant information about the proposal. The Office of Access Card website has little more than simple 'fact sheets'.

Details about the proposal must be drawn, with some significant effort by the keen researcher, from a mixture of sources, such as the publicly available extracts from the KPMG Report, Hansard of Senate Estimates hearings, Ministerial press releases and speeches, and the Taskforce's own Discussion Paper. In several instances, these differing sources are contradictory, confusing or misleading.

The Government is able to distance itself from each of these sources as it desires, and indeed has already done so in relation to the KPMG Report (and the unreleased Privacy Impact Assessment), such that it is almost impossible for anyone outside the Government to get a 'handle' on exactly what is or is not proposed at any given time.

That the Taskforce should have been left to attempt to describe the Government's initiative is particularly concerning, as one is left with the impression that the Taskforce is expected to 'sell' the proposal on behalf of the Government.

Our understanding of the proposal arises from careful research of available materials and is described, together with our concerns, in our information paper *What we do (and don't) know about the proposed 'Access Card'* – see Attachment A.

Not enough transparency

We repeat our demand for the release of the privacy advice, including the Privacy Impact Assessment (PIA), commissioned by the Government to examine the privacy implications of the proposal at the same time its potential benefits were being examined by KPMG.

We utterly reject the notion that the PIA is 'redundant' because the proposal has in some undefined way 'moved on' since the PIA was written. If that is true of the PIA, then it is also true of the KPMG report, and thus also true of the value proposition, estimated costs and estimated benefits on which Cabinet and Treasury approval rests.

We also reject the Government's argument that the PIA and unpublished parts of the KPMG Report are 'cabinet-in-confidence'. This is of course entirely in the Government's hands. If some parts of the KPMG Report can be published by the Government, then all parts can, and the same applies to the privacy advice.

We also do not accept the Government's arguments that details of how the system would work cannot be released because they would affect the tendering process. This is unjustifiable, since tenderers will need to see detailed specifications in order to prepare their tender. If all the information is released to the public at the same time, then no one tenderer will be advantaged over another.

The privacy advice must be publicly released, along with the draft design documents, to give the public an opportunity to make fully informed judgments about what level of privacy protection they find acceptable. Proposals can only be improved by throwing the design and underlying assumptions open to robust public scrutiny and debate.

If the Government is genuine about wanting to listen to and address privacy concerns – rather than just 'manage' them – then the Government must be open about the privacy implications of its proposal, and let the public make up its own mind about whether it accepts those implications.

Not enough time

The Minister's desire to start issuing cards as soon as 2008 suggests undue haste, particularly when one considers the scope and breadth of this project, and its potential impact on the life of every Australian. This haste not only greatly diminishes the project's likelihood of staying on time and within budget, but also forces truncated consultation and design phases.

Though this ridiculously short timeframe is not the fault of the Taskforce, the Taskforce's plan to issue its first report to the Government in October 2006 – after lead advisers and project managers have already been appointed and working for several months with a deadline of 2008 for implementation – suggests the result of public consultation may come too late to have significant impact on key decisions.

We suggest the Government would do well to take a deep breath and let go of its 2008 'deadline', and instead allow the proposal to unfold in enough time to allow genuine public consultation and input, before design specifications are even contemplated, let alone implementation begun.

In particular, it is very difficult to have confidence in the likelihood of any privacy 'add-ons' being effective, once the Government has committed to a specific technology model. Privacy needs to built-in from the beginning, not tacked-on after the design phase.

Privacy concerns treated in tokenistic way

We believe the language of the KPMG Report says it all about the Government's attitude to privacy concerns.

Privacy is described in the KPMG Report as a concern to be 'dealt with', as a set of 'issues which need to be managed', as concerns to be addressed at 'the implementation stage and thereafter', or as a subject of 'reassurance' as part of the communications strategy - rather than actually *resolved*, by way of building-in privacy protections during the planning and design stages (KPMG Report, pp.3, 13, 28, 32).

That the Government has refused to release the PIA it commissioned only lends further weight to our suspicion that the Government is burying its head in the sand on genuine concerns from the public, believing that some PR 'spin' about the benefits of the card will somehow nullify privacy concerns.

What is of great concern to us is that there appears to be no recognition, either by KPMG or the Government, that privacy considerations need to be built-in at the planning and design stages of the project, not just 'managed' through a

'communications strategy' at the implementation stage, when it is too late to change the design specifications.

While the appointment of the Consumer and Privacy Taskforce can be seen in one light as a positive step towards addressing consumer and privacy concerns, in another light one can see that perhaps the Government is just using the Taskforce as a filter, to maintain its distance from any direct engagement with consumer and privacy perspectives – yet all the while dealing directly with banks and the smartcard industry.

A hamstrung Taskforce

The manner in which the Taskforce has been established also suggests that consumer and privacy concerns are seen by the Government as a PR nuisance, instead of what it is: a core issue to be engaged with, critical to the proposal's success - or failure.

While the Minister has described your Taskforce as 'independent', he has not guaranteed you the conditions of independence through the normal arrangements one would expect, such as fixed terms, appointment by the Governor General rather than the Minister, removal by the Governor General only in grounds of incapacity or corruption, a separate budget under your own control and discretion, formal terms of reference, and statutory powers to demand information and directly publish your views.

Furthermore the location of your Taskforce as part of the 'implementation group' within the Department of Human Services, the presence of a self-declared Departmental representative on the Taskforce, and the ridiculously short timeframe for the Taskforce's initial work, also suggest the Government is not genuine in its desire to obtain comprehensive and independent advice.

Given this situation, we are concerned that the Government sees the purpose of the Taskforce as just to smooth the passage of the project, and lull Australians into a false sense of security, rather than to genuinely facilitate input into the design process or speak on behalf of the public interest.

We urge you to use whatever means at your disposal to ensure that the work of the Taskforce is not misused.

We also urge you to contribute to the transparency of this project by publishing all submissions made to you[1], and publishing all reports or advice you give to the Government.

[1] We note that your Discussion Paper, in calling for submissions, does not address the issue of confidentiality and/or publishing of submissions. We suggest that where a submission's author has not made their views on publication of their submission already known, that you contact them to seek their views.

The project's rationale, claims and scope

The Taskforce must review claims about benefits

While the Taskforce has not sought to examine the claims made by or for the Government in relation to the estimated costs and benefits of the so-called Access Card, we submit that in order to assess the implications from a consumer and/or privacy perspective, these claims *must* be examined.

If the estimated financial benefits are not realised, then the justification for the expenditure of billions of dollars is lost. Nor can interested parties, and the public at large, weigh alleged consumer 'convenience' against the potential negatives – such as privacy invasive impacts – unless the claims about both have been tested.

We have doubts about many of the claims made about the alleged consumer benefits to be derived from this project. Perhaps most importantly, we would make the point that if all the 'consumer benefits' of the card are so self-evident and self-justifying, there ought be no need to make the card compulsory to access any health or social service benefit.

The fact that the proposal is for a de-facto compulsory card (which you acknowledge in your Discussion paper) suggests that the 'benefits' do not actually stack up against the downsides for the average 'consumer'.

The claims or implicit assumptions that we doubt, and which we recommend that the Taskforce review, are as follows (page references are to our *Information Paper* at Appendix A):

Consumer benefits

- That any significant benefits will be delivered to the 50% of adults who are not clients of Centrelink or the DVA (see p.9)
- That a smartcard is needed to deliver the benefits of 'single customer record' (to enable a single 'change of address' notification for example) (see p.10)
- That consumers will experience significantly different, faster or better service delivery (see pp.11-12)
- That some of the 'optional extras' such as storing emergency contact and health information could not be better achieved without linking through a smartcard to a centralised database (see p.13)

Combating fraud

- That the $3 billion in welfare fraud savings estimated by KPMG can actually be attributed to the so-called Access Card initiative alone (see p.14)
- That the introduction of a de-facto national ID card will reduce identity fraud (we actually believe it will make the problem worse) (see p.15)
- That the scope of welfare fraud, which appears to be concentrated in Centrelink programs, necessitates a universal card issued to the 50% of adults who are not clients of Centrelink or the DVA (see p.15)
- That any fraud-related savings cannot be achieved in any other, less privacy intrusive way (see p.16)

- That claims made about abuse of concession entitlements are valid (see p.18)
- That this proposal will address or 'fix' abuse of concession entitlements (see p.19)
- That this proposal will resolve the problem of data accuracy (see p.19)

The Access Card – trying to be all things to all people

We see some of the objectives of the so-called Access Card as ill-defined and pretty flimsy. Indeed much of the public discussion to date has focused on the more 'fringe' applications that are nonetheless populist and therefore easy to 'sell', such as emergency relief in the wake of Cyclone Larry, storing emergency health information, and creating a "high value" photo ID card suitable for businesses to use.

The Minister has also hinted at the card's use for electronic prescriptions, while others have suggested it also be used for full electronic health records, regular social service payments (with limits on how that money can be spent), and controlling access to child-care centres.

If the Government is genuine in its desire to improve 'access' to health and social services, then it must remain focussed on that task. If the Government is genuine in desiring that its so-called Access Card not become a de-facto national ID card, then it must drop some of these superfluous functionalities. Emergency health information is the job of the Health Minister; and given the Government's assurances a role for the card as an all-purpose ID document ought not to be in scope at all.

The internal wranglings evidenced in the KPMG Report over what to do with people who cannot meet the threshold requirements for 'gold standard' proof of identity, but who nonetheless should be entitled to Medicare and other health and social services, highlights the catch-22 situation the Government has created.

There will be various communities of people who will not be able to meet the minimum standards of registration information needed to obtain an Access Card; these are most likely indigenous people, the elderly, homeless, refugees, and people with disabilities.

KPMG recommended that people who cannot meet the minimum standards of registration information should still be issued with a card, but that the card have a "low POI confidence flag" (KPMG Report, p.52).

If the 'low POI confidence flag' is printed on the face of the card, it would likely lead to (or entrench) discrimination against these already-disadvantaged people. In effect, some people would be flagged as second-class citizens.

However if this 'low POI confidence flag' is only held on the chip (as the KPMG Report recommends, p.52), it will require third party users of the card to all have a card reader, to test whether the Government is confident enough about each card holder's identity to not issue a 'low POI confidence flag', before they rely on the card as evidence of that person's identity.

This has two implications: firstly, the alleged 'privacy enhancing' nature of the card, as a useful 'proof of ID' card with limited extraneous information on its face, is shown

to be false – the extra information will simply be read from the chip instead; and secondly, the argument about the card number needing to be on the face (or back) of the card is also shown to be untrue.

The net result is that the Government is unable to deliver on one of its promises to deliver a simple 'proof of ID' card for people who suffer now from the lack of a photo ID card because they don't have a driver's licence. The card could only work as a 'proof of ID' card when read in conjunction with information stored on the chip, which opens the door to a far more privacy-invasive (and expensive) model of ID card than we have been promised to date.

This suggests to us that the Government should drop this proposed 'all-purpose ID' function of the card, and dramatically scale back the proposal to being a card that is only ever to be used to obtain DHS or DVA benefits.

As one Government backbencher has already said, if this is supposed to be a card to improve access to DHS and DVA services, then the only time it should be used is to access DHS and DVA services – end of story. Instead, we have a Government intent on propping up its 'business case' for the card by selling the public on a range of fringe applications, the viability and business cases for which appear not have been established.

Unless this proposal is significantly reined in, the privacy implications will so far outweigh any alleged benefits that, we believe, the proposal must be opposed outright.

Identity issues

A national ID card

The 'Access Card' proposal, as it exists now, would create a national ID card scheme, very similar to the 'Australia Card' proposal of the 1980s. (See Appendix B for a table-format comparison with the Australia Card proposal.)

The 'Access Card' is much more than just an extra card in our wallets, and much more intrusive than the systems it would replace.

A national ID number

What is most significant and different about the 'Access Card', as opposed to a driver's licence or a passport, is that the card number creates a single key, through which both governments and businesses can confidently index, link, track and profile our movements, transactions, and personal affairs, combining records in large scale and routine ways.

This type of linking and profiling is not currently possible, because Australians do not have assigned to them a single, universal and unique number. Drivers' licences and passports are not universally held; Medicare card numbers are not unique as they can cover more than one family member, and tax file numbers must be kept confidential by the organisations that are permitted by law to collect and use them. The 'Access Card' proposal introduces a single, universal and unique number for every person – in effect, a national ID number.

The creation of a national ID number means governments and businesses can not only identify people at the time of a transaction, but can also link their records with information about the same people collated from other organisations, and thus build up profiles of our activity.

So while many Australians might not mind showing some form of evidence of identity each time they board a plane, mail a parcel overseas, visit a doctor, write a cheque, fill a prescription, apply for social security payments, rent a car, buy a concession train fare or open a bank account, the idea that all those aspects of our daily lives might be tracked, linked together, matched and profiled - and the resulting profiles used to make decisions about us - is far more disturbing.

The potential for abuse of this indexing, linking, tracking and profiling capability – and indeed the specific memory of abuses by various totalitarian regimes in our lifetime - is why the development of unique and universal identification systems has been prohibited under the constitution of some countries, and under general privacy laws in others.

A national ID card would profoundly affect the everyday lives of Australians. The mass 'dataveillance' system it represents would treat all Australians as suspects, instead of free citizens.

The end of anonymity

Anonymity in our daily lives is necessary if we are to protect freedom of speech, and freedom of association. Yet the very creation of a universal ID card strips away from people the ability to be anonymous. There will no longer be a perfectly valid

explanation ('I don't drive') for why a person does not have a photographic identification document handy at all times.

Overseas experience tells us what happens next. Providers of goods and services know that their clients or customers no longer have a 'real' excuse for not having photo ID, and so they will start demanding photo ID in more and more routine transactions.

We would quickly reach the stage where someone who does not produce their card on request will be viewed as inherently suspicious. This is particularly troubling when the Government is encouraging ordinary citizens to report any behaviour or activity that seems out of the ordinary.

Yet respecting privacy is about recognising that all of us have a space in our lives we prefer to keep private. That does not mean we have 'something to hide'.

We don't disclose to strangers our bank account numbers or PINs, because we want to protect our finances. We may choose to protect information about our health, sexual activities or religious beliefs, because we wish to avoid embarrassment or discrimination. Sometimes we just want to avoid unnecessary intrusion, harassment or solicitation. And there are many people at threat from harm, for whom keeping their address or movements secret is a matter of personal safety.

Impact of the proposal on identity fraud

A national ID card scheme, which the access card proposal amounts to, poses a threat not only to our privacy and anonymity, but to our personal information security.

Identity fraud and identity theft can be used to support a wide range of illegal behaviour – from under-age drinking, through welfare or benefit fraud, to the adoption of false identities to assist in organised crimes including terrorism.

Yet the introduction of a single, universal identity document just raises the stakes. As the Attorney General has noted, a national ID card 'could increase the risk of fraud because only one document would need to be counterfeited to establish identity' (Philip Ruddock, 29 June 2005, Australian Smart Cards Summit).

Furthermore the 'Access Card' is proposed to link to a massive and complex system featuring a centralised, national population database – the proposed SCRS.

However this centralised database of personal information would likely make identity fraud and theft *worse*. This is because of a centralised system's vulnerability to hacking, manipulation and corruption. Indeed, when speaking to the AusCert security conference in May 2006, the Deputy Commissioner of Taxation warned that the 'Access Card' proposal, if implemented, would lead to a *rise* in identity theft.

The proposed national population database, the SCRS, would not be any more secure, free from corruption or immune from simple clerical errors than any other database. The use of biometric photographs could indeed prove disastrous, as the victim of identity theft or data corruption cannot just be issued with a new face.

Experts at the Homeland Security Summit, held in Canberra in the wake of the London bombings in July last year, identified a range of targeted activities which could be undertaken to prevent or lessen the effects of terrorism, including better

resourcing of intelligence services, police training, and development of response plans. We know of no expert advocating ID cards as a genuinely effective tool in fighting terrorism. Indeed many terrorists do not hide their identities. The then UK Home Secretary Charles Clarke admitted national ID cards would not have prevented the London bombings.

The National Identity Security Strategy, announced in May last year, also recognises that our current system of multiple identity documents should be strengthened, not replaced, in order to tackle identity fraud and the crimes it supports.

A national ID card would cost Australians billions of dollars that could be better spent on real solutions to identity fraud and the crimes it supports – or on improving the health and welfare sectors in more meaningful ways.

Alternative models - what should be considered

We urge the Taskforce to review alternative models for delivering on the promise of better access to social services, and, separately, access to *health benefits* (as noted above this card will NOT affect access to *healthcare*, except in relation to the ill-conceived proposal for emergency information).

As a minimum, any new Medicare card (a near universal entitlement) must be kept separate from any card for which eligibility is not universally available to Australian citizens and permanent residents. Administration of health benefits unavoidably involves information relating to health care delivered, much of which is highly sensitive. It is for this reason that health administration information has been subject to specific privacy rules designed in part to quarantine it from other areas of public administration. The use of Medicare and Pharmaceutical Benefits Scheme information is currently subject to detailed restrictions under the National Health Act, and several States and Territories have enacted specific health privacy legislation. Consideration is being given to a National Health Privacy Code – the slow development of which reflects the complexity and sensitivity of privacy rules for health information. The proposed inclusion of Medicare and PBS in the Access Card proposal threatens to overturn a decade or more of carefully constructed rules.

We provisionally support the following approaches to the targeted application of smartcard technology within these two distinct and separate areas of public administration – social services and health. They are not all alternatives; nor are they mutually exclusive.

- Upgrading the near-universal Medicare card, if necessary, to a smartcard, with *either* name or photo on the face of the card (not both) – but maintain this as separate to any other DHS or DVA card, or any other agencies, initiatives or benefits
- Having a separate 'proof of entitlement' card for people entitled to one or more DHS / DVA-issued concessions, with a name or photograph (but not both) on the face of the card, and current concession status on the chip of a card, but maintain this as separate to the Medicare card; and legislate to only allow people to ask to see or check the card where the person is seeking a concession benefit or discount
- Taking the ID number off the face (back) of any DHS / DVA-issued card, and replacing it with a simple expiry date for the card
- Taking the photograph off the face of any DHS / DVA-issued card, but making the photo readable from the chip for authorised people (relevant DVA and DHS staff, and health service professionals providing a DHS / DVA-related benefit)
- Alternatively, leaving the photo on the face of any DHS / DVA-issued card, but taking off the name – such that the mere existence of a person who matches the photo on their card means the carrier is entitled to the service, with all other entitlement and customer information to be on the chip instead

In any scenario, there should be legislation to prohibit anyone but an authorised person from ever asking to see, copy or download information from any card.

It's not just about the ID card - other privacy and data security concerns

Our Information Paper at Appendix A covers a range of other privacy and data security concerns, which we submit the Taskforce must examine, including:

- The deletion of information from the SCRS for individuals 'leaving' the system, for instance by opting out of entitlement for benefits or permanently leaving the country (see p.21)
- The prospect of 'identity denial' or second-class citizenship for disadvantaged people (see p.28)
- The potential for innocent people to be falsely accused of identity fraud because of the high error rates in facial recognition (see p.30)
- The likely disproportionate impact of facial recognition errors on people with disabilities, the frail aged, indigenous and homeless (see p.31)
- The storage of excess information in the card's chip (see p.33)
- Who will be able to read the chip's contents, in what circumstances (see pp.34-40)
- Whether people will be able to suppress their home address and other details on the chip (see p.34)
- What standards will be used for the chip? (see p.35)
- The storage of excess information in the SCRS (see p.47)
- The necessity of storing actual photos and signatures as well as their biometric templates (see p.47)
- Whether people will be able to suppress their home address and other details on the SCRS (see p.47)
- How long information will be kept on the SCRS (see p.48)
- The scanning and storage of people's 'foundation documents' (see p.48)
- Who will hold and manage the SCRS (see p.48)
- Who will have access to the SCRS, in what circumstances (see pp.48-51)
- How else the data on the SCRS might be used, or what it might be matched or linked to (see p.51)
- The arrangements in relation to data security (see p.51)

International experience

The Government has been keen to selectively use experience in other jurisdictions in support of its case for the smartcard. We urge the Taskforce to conduct a more objective review of international experience, both of relevant smartcard and biometric technology and of Identity Card systems. In particular, we suggest close scrutiny of the current UK ID card initiative, where many of the UK Government's claims appear to have been discredited and there are significant doubts about the technical assurances and cost estimates.

We again emphasise the importance of the Taskforce seeking independent evaluation of the Australian Government's business case for the 'Access Card', as it is a fundamental requirement for any assessment of the privacy impact to be clear about the benefits which we are being offered to offset any loss of privacy.

APPENDIX A

Information Paper "What we do (and don't) know about the proposed 'Access Card'"

See separate document.

Available at http://www.privacy.org.au/Campaigns/ID_cards/HSAC_Info_Paper.pdf

APPENDIX B

Spot the difference: national ID card proposals

Australia Card 1986 – 87 *vs.* Access Card 2006 – ?

What makes a national ID card system?

☑	A unique ID number for every person	☑
☑	Scheme is national, covering effectively every man, woman and child	☑
☑	Adults will be issued with a card, showing their photo	☑
☑	A national ID number is included on the card	☑
☑	A national population database will hold names, date of birth, photos, ID numbers and addresses of every adult	☑

What else has been proposed?

☑	Compulsory for access to Medicare	☑
☑	Compulsory for claiming social security benefits (like the 'baby bonus', carer's allowance, pension, Austudy or disaster assistance)	☑
No	Compulsory for claiming Veteran's benefits	☑
Not invented yet	A computer chip in the card to store extra data	☑
Not invented yet	A biometric photo (facial recognition technology)	☑
☑	A compulsory registration process: every adult required to turn up, show their papers and be photographed	☑
☑	The same agency responsible for Medicare will also hold the national population database	☑
☑	Not required by law to carry it – but in practice you'll have to	☑
No	Promoted as an all-purpose 'proof of identity' card	☑
☑	Businesses and government agencies can ask to see your card if they want evidence of identity	☑
☑	Police and other law enforcement agencies to have access to the database (no special protection)	☑