



**Australian
Privacy
Foundation**

GPO Box 1196
Sydney NSW 2001

www.privacy.org.au

28 February 2007

Committee Secretary
Senate Finance and Public Administration Committee
Department of the Senate
BY EMAIL: fpa.sen@aph.gov.au

Inquiry into the Human Services (Enhanced Service Delivery) Bill 2007

Dear Senators,

We are pleased to make the attached submission, and ask that you carefully consider the issues raised.

This submission is not intended to replicate the substantial work of analysis by other parties, but to flag the essence of a range of the most serious concerns held by a number of organisations and individuals.

This submission is therefore intended as a summary of issues we seek to elaborate on verbally. We would be pleased to have a campaign member elaborate on these comments in person, and therefore request the opportunity to present a verbal submission at the Committee's hearings in March.

To arrange a time for a verbal submission, please do not hesitate to contact me on (02) 9432 0320 or 0400 432 241.

We consent to (and indeed encourage) publication of this submission on the Committee's website.

Yours sincerely

Anna Johnston
No ID Card Campaign Director,
Australian Privacy Foundation

Submission on the Access Card proposal, and associated legislation

Contents

About the Australian Privacy Foundation.....	1
The scope of the proposal.....	2
It is an ID Card	4
The safeguards are inadequate.....	5
The costs outweigh the savings	7
The risks outweigh the benefits	8
Social impacts on the disadvantaged	10
Conclusions	11

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 our formation in 1987, to fight the ‘Australia Card’ proposal, 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.

The No ID Card campaign is co-ordinated by the Australian Privacy Foundation, but draws on the assistance of a number of other, unrelated non-government organisations and individuals. The No ID Card campaign seeks to raise concerns range across a number of areas, including social justice impacts, waste of public money, and the impact on personal privacy.

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

The scope of the proposal

We do appreciate that the terms of reference for this Committee only extend to reviewing the Human Services (Enhanced Service Delivery) Bill 2007.

However we respectfully request that the Committee take a holistic view of the legislation. This one Bill cannot be considered in isolation from what Bills are also intended to follow, nor in isolation from the Access Card proposal as a whole.

Many of the fundamental aspects of the Access Card scheme are not covered by this Bill. The Bill is silent on almost all permitted or prohibited possible uses of the card, or the permitted or prohibited uses of the data, including biometric photographs, to be held in the back-end national population register. We do not accept the Government's promises that later legislation will deal with prohibitions on use of information from the register¹

The Bill is also silent on how the smartcard infrastructure may be used by the banking or retail industries, yet the scheme's Chief Technology Architect is due to explain to an industry summit in late March how the card could become the "common railroad" for retail in Australia². Australians deserve to know whether the Access Card scheme is effectively a taxpayer subsidy for the banking and retail industries, which have not otherwise seen the business case for adopting smartcard technology.

It is outrageous to expect the public or Parliament to accept \$1.1 billion in expenditure, without the Government first showing the public all the details of the scheme. We suspect even more intrusive and disturbing aspects of this proposal to only emerge after tenders have been signed, and this first Bill has been passed.

In particular, we are horrified at the poor governance and project management evident in the handling of this proposal, in which the Government has already requested tenders, worth tens of millions of taxpayers' money, before either allowing the finalisation of the Consumer and Privacy Taskforce's public consultation process, or being sure its legislative framework will survive Parliamentary scrutiny.

¹ This Bill goes into similar levels of detail about the contents of the register as it does about the contents of the card, so statutory interpretation would suggest this omission is significant and could be expected to imply there is no intention for there to be such protections for the register, leaving it entirely open to abuse.

² Conference program for *Cards & Payments Australasia 2007*, 27-28 March 2007, Amora Jamison Hotel, Sydney.

No doubt the Government will seek to scare opponents into supporting the legislation, on the basis that its own mismanagement of the tendering process could expose taxpayers to millions of dollars in liabilities, should details of the scheme now be changed by Parliament. We urge you to resist such pressure - neither Parliament nor the Australian people should be blackmailed into supporting this scheme.

It is impossible for the Senate to evaluate, from the current Bill alone, the full legal structure intended to support the Card system, including the adequacy of legal protections. We therefore urge the Committee to recommend halting Parliamentary debate on the Bill, and any further tendering or awarding of contracts by the Government, until such time as all the currently suppressed reports on privacy and costs are released, the public consultation process is complete, the design specifications are complete, and *all* related legislation is ready. Only then can the full implications of this Bill be considered properly, in the appropriate context.

It is an ID Card

Despite the Government's claims to the contrary, the Access Card *is* a national identity card. Its design goes beyond what is strictly necessary for accessing health and welfare benefits, and the legislation is so weak as to allow – and in some cases facilitate - a wide range of uses, entirely unrelated to health or welfare.

The Government has described the Access Card as an “identity tool”, and as providing a “high value proof of identity” – yet balks at the phrase “ID card”. Notwithstanding the Bill's strange but ineffective assertions to the contrary, the difference is purely semantic.

The Access Card will introduce, for the first time in Australia's history, a universally-issued card, which features a unique number, name and biometric photograph. (Current Medicare ‘family’ cards are not unique to the person; passports and driver's licences are not universal; and the Tax File Number is not printed on a card for your wallet.)

Furthermore the register that sits behind the card will be a national population database, holding a unique ID number for every person (including children), an unprecedented set of biometric photographs of every adult, and personal data like home address, and the links between family and former family members.

The design of the Access Card scheme supports data-matching, profiling and the creation of virtual ‘dossiers’ on all Australians, of an unprecedented degree and scope. Although this invisible functionality is hidden in the ‘back room’ database, its unchecked proliferation is one of the main privacy dangers of the proposed Access Card system.

The safeguards are inadequate

The Bill fails to delineate either a set of permissible uses, or a set of clearly prohibited uses, of the card, of information held on the card's chip, or of information held in the central database.

The Bill's supposed protections against the card's use as an ID card are a transparently weak fiction, with six loopholes:

- Crown immunity
- the card can be used as proof of ID if the person so "chooses"
- the card can be requested as ID – it just can't be "required"
- copying information from the card is allowed with the person's "consent"
- other legislation will override this Bill, and
- the protections do not apply to information found only on the card's chip.

Officials across all three tiers of government – from police officers to bus drivers to social workers - will be able to demand the card as proof of ID, as clause 9 of the Bill provides Crown immunity from the Bill's criminal sanctions, which are the only form of restraint on use in the Bill with even limited effectiveness. Indeed, Immigration officials have already suggested the card could be used to identify missing or detained persons – a purpose unrelated to the delivery of health or welfare benefits.

Card holders will not be prevented from using their card as a form of ID, because under clause 40, you may "choose" to use it for this purpose.

Under clauses 45-46 of the Bill, private sector organisations will also be able to "ask" people to show their card as proof of ID, or as a precondition to entry to premises, or the supply of goods or services, just so long as they don't "require" it. Banks already plan to use the Access Card as part of the '100 points of ID' system to monitor financial transactions.

Under clause 57(2) the Bill, anyone will also be able to copy, use and disclose your unique ID number, photograph or signature, so long as they have your written consent. We imagine that your "consent" will very quickly be written into the application form for every bank account, video rental store card, RSL club membership, retail loyalty card - and job³. Once an organisation has

³ We expect the private sector and government agencies to abuse the rhetoric of 'choice' and 'consent' to make use of the Card more or less ubiquitous, even though such 'consent' will likely be neither properly informed nor truly voluntary.

logged your universal, unique ID number, it can use that number to track, data-match and profile otherwise unrelated, disparate pieces of data about you⁴.

In any case, as noted in the Bill's Explanatory Memorandum, other laws such as the new anti-money laundering laws, which require the copying of unique identifiers such as Access Card numbers from the customers of a wide range of institutions, will override the offence provisions in this Bill⁵. In such circumstances, written consent will *not* be needed to copy, use and disclose your unique ID number, photograph or signature, so long as the Access Card is handed over by the "choice" of the customer in the first place.

Furthermore, the Bill does not prohibit copying or maintaining a record of information taken from the chip in the card, so long as that information is not also found on the surface of the card⁶. Clause 57 of the Bill therefore does not prevent any person from copying and maintaining a record of the chip's unique serial number, which is not encrypted, cannot be protected by a PIN, and is readable by any person with a standard smartcard-reader⁷. This is effectively a second, covert unique identification number that can be copied, used and disclosed – all hidden from the view of the card-holder.

We are appalled that card-holders who trust the Government's promises will be lulled into a false sense of security, believing that when they 'choose' to hand over their card as proof of ID, their ID number cannot be recorded or used without their written consent. However this will not be the case in so many circumstances, making the Government's promises so meaningless as to be positively misleading.

⁴ Although we are told the number on the card will be a card number, separate to the lifelong unique ID number to be held in the underlying database, for most purposes the card number will be useful for these data-matching purposes, as we understand the intention is for people to retain their card for many years. Furthermore we do not see any safeguards in the Bill to prevent consecutive cards featuring consecutive card numbers, as Medicare cards do now. (Upon renewal the Medicare card number only alters by one digit – the final digit is increased by one.)

⁵ The *Human Services (Enhanced Service Delivery) Bill 2007 Explanatory Memorandum*, p.53, states: "Section 10.5 of the Criminal Code provides that a person does not commit an offence under a Commonwealth law if the person's actions are justified or otherwise excused under a law of the Commonwealth. For example, under section 108 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* reporting entities are, in certain circumstances, required to make and retain a copy of a document used for identification purposes. In a situation where a person chooses to provide their access card to a reporting entity (e.g. a bank), the entity would in certain circumstances be required under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* to make and retain a copy of the card (which would include the card number). In this situation section 10.5 of the Criminal Code would apply and the reporting entity would not be criminally responsible under clause 57."

⁶ The prohibition against copying, recording or disclosing information only relates to "the access card number, photograph or signature on the surface of an access card" – see cl.57(1)(a) in the Bill.

⁷ Smart cards each contain an integrated chip with a unique permanent identification number, burned-in during the manufacturing process – the Card Serial Number. The Card Serial Number is not encrypted and can be read by any ISO-compliant reader. For more see the website of Software House, a supplier of smart card readers:

http://readers.swhouse.com/pages/Smart_Card_Overview.aspx

The costs outweigh the savings

The cost of the Access Card system has been budgeted at \$1.1 billion over four years from July 2006. We all know complex IT projects tend to run well over budget⁸, and this project will be no exception. (Even the development of the initial business case⁹ by the accountants KPMG ran \$200,000 over budget!)

KPMG also estimated the cost of health/welfare benefits fraud and other 'leakage' from the health/welfare federal budget as being between \$1.6 and \$3 billion over 10 years from July 2010. However, because the details remain suppressed, it is hard to drill down to see the basis for these claims.

From what we can see of the KPMG report, it does not actually promise that all this fraud or 'leakage' will be prevented by the Access Card¹⁰. The Access Card will do nothing to stop entitlement-based fraud, such as people understating income or assets – a far more common type of fraud than identity-based fraud. Nor will the Access Card resolve all elements of human error.

Even if the Access Card miraculously only costs \$1.1 billion to roll out, and \$1.6 billion was saved as a result after 14 years, the return on investment is less than 3% p.a. The money would be better off in the bank! If the Government really wanted to improve access to health benefits, it could perhaps spend the \$1.1 billion on universal dental care – or 11 new hospitals.

⁸ Typically 75% of IT projects do not deliver usable outputs on time and on budget, so given the growing number of IT project management disaster warning bells already going off, we expect the Access Card project to fall into that category.

⁹ Despite repeated requests, the details of the KPMG report which would have enabled a more in-depth assessment of the cost / benefit analysis remain suppressed, as does the Privacy Impact Assessment which presumably sets out many of the other costs and risks to individuals and small businesses.

¹⁰ The language in the KPMG Report is a little hazy on this point. It doesn't actually make the direct claim that the Access Card proposal will generate \$1.6 to \$3 billion in financial savings for the Government. It is not clear whether the claimed \$1.6 to \$3 billion in savings relates only to this so-called Access Card initiative, or to the sum total of savings that could be achieved if all fraud was resolved: "KPMG have provided ongoing advice to the Australian Government that fraud savings could range from at least \$1.6 billion to \$3 billion over a ten year period" (KPMG Report, p.12). Details are not provided of where those savings will come from.

The risks outweigh the benefits

If the 'consumer benefits' of the Access Card were genuinely worth it to the individual, there would be no need to make the card compulsory for accessing Medicare and other Government services.

Indeed many of the claimed 'consumer benefits' are being over-sold, because we don't need the Access Card to deliver them; in many cases, it's not even clear how the Access Card *could* deliver them:

- a single 'portal' for across-Government change of details is already being worked on now
- Medicare 'swipe and go' rebates at the GP's desk are coming in 2007 anyway, through the EFTPOS network (indeed some are already up and running)
- storage of e-health details: health consumers and clinicians have questioned the sense of this proposal, when a similar model has been promised and failed three times before (the MediConnect, HealthConnect, and Tasmanian Medicare smartcard trials); pre-existing, cheaper and less risky models are already available¹¹; and development of the infrastructure to facilitate a national shared e-health record is a complex, long-term, multi-jurisdictional task, now with the National E-Health Transition Authority
- delivery of emergency relief: there is no discussion in the KPMG business case about how the Access Card is supposed to work in situations such as cyclones when there is power failure.

About the only 'benefit' to the individual is combining several cards into one. However only very few people currently hold more than 3 or 4 of the 17 cards to be 'combined'. There is **no benefit to the majority** of Australians, who only hold a Medicare card now.

Yet the risks caused by this proposal will rise for every Australian – the risks of identity theft and fraud.

The Access Card is intended to be issued on a universal and unique basis; that is, one card per adult, and, unlike the current Medicare cards, only one person per card. The card number, to be printed on the surface of the card, thus uniquely identifies the person named on the card. Furthermore, the card's unique serial number, to be held on the chip of the card and potentially

¹¹ The Medic Alert system, health alert bracelets, the national organ donor register, and even a home-made piece of laminated paper kept in your wallet with emergency health and contact details, are all available now.

also on the national population database¹², will be unencrypted and readable by any person with a standard smartcard-reader¹³.

The notion of a single ID card, ID number and/or ID database is contrary to the National Identity Security Strategy. Such a system places all our identity eggs in the one basket – it means only one document needs to be forged, or obtained illegally, through bribery or hacking, to steal someone else’s identity, or create a new fake one. Senior officials at both the Taxation Office and the Australian Institute of Criminology have said that the Access Card will lead to *increased* identity theft, not less.

Furthermore, introducing the Access Card before the problem of fake foundation documents (birth certificates, passports, etc) has even begun to be tackled is like presenting a gift to organised criminals and terrorists. The more sensible Document Verification System, which aims to identify fake foundation documents, is not scheduled to be operational until at least 2010 – by which stage the Government will have allowed perhaps tens of thousands of fake identities to be entrenched and thus ‘legitimised’ in the Access Card system.

Additional risks arising from the adoption of a single ID number include the proliferation of dossiers and data mining networks across governments and the private sector, as has occurred in the USA through extensive use of their Social Security Number for unrelated purposes.

One over-arching question is why so much data needs to be on a simple but vulnerable card, when most core benefits payments are administered by massive national computer networks. A much simpler card could omit much of the data, and therefore reduce many of the risks.

¹² The Table at cl.17 of the Bill sets out the contents of the national population database, the Register, which will underpin the Access Card system. Item 17(a) in the Table provides that the Secretary of the Department will be able to add the chip’s serial number to the Register.

¹³ Smart cards each contain an integrated chip with a unique permanent identification number, burned-in during the manufacturing process – the Card Serial Number. The Card Serial Number is not encrypted and can be read by any ISO-compliant reader. For more see the website of Software House, a supplier of smart card readers: http://readers.swhouse.com/pages/Smart_Card_Overview.aspx

Social impacts on the disadvantaged

There is no evidence that the Access Card will actually improve anyone's access to health or welfare benefits. Indeed the main immediate impact will be the diversion of at least \$1.1 billion from the provision of desperately needed real services into the hands of the IT vendors, lawyers, consultants and advertising agencies feeding off this project.

In fact this proposed regime is more likely to make access to health and welfare services more difficult, especially for those who lack the necessary foundation documents to re-prove their identity to the Government's new standards. This will likely entrench social disadvantage for Indigenous people, the homeless, people with disabilities, and people of a non-English speaking background.

One option on the table, according to the KPMG report, is to still issue cards to such people, but with a flag indicating 'low confidence' in their identity. To be effective, such a flag would need to be visible on the surface of the card. This looks to us like branding some Australians as second-class citizens. The Access Card is only likely lead to service denial and identity denial.

There is also scope for profiling and other forms of information abuse on the basis of this 'low confidence' flag, Aboriginality and other data items.

Conclusions

The Senate is being asked to pass legislation before all the details have been worked out in other fora; meanwhile the Government is preparing to receive final tenders on the same day this Committee is due to report, on the assumption there will be no amendment to the legislation.

Regardless of what one thinks of the merits of the Access Card scheme, this is negligent project management and suggests the Government is treating both the Senate, and the Australian public, with contempt.

We therefore urge the Committee to recommend to the Senate that the Human Services (Enhanced Service Delivery) Bill 2007 be rejected as unjustified, unworkable, inadequate, and a potentially costly and stupid mistake, for the following reasons:

- all major political parties, including the Government, have indicated their opposition to a national ID card, and public opinion polls suggest Australians' opposition to ID cards remains high
- yet the Access Card scheme will be a national ID card scheme – by design and effect, if not by intention
- the privacy safeguards in the Bill are woefully inadequate, with six loopholes already evident
- the costs will likely outweigh the benefits
- the risks will likely outweigh the benefits, and
- the scheme will further entrench social disadvantage for the most vulnerable Australians.

In the alternative, we urge the Committee to recommend to the Senate that, at the very least, debate on the Bill should not commence until:

- all Access Card-related Bills, and subordinate legislation, are available for review as a single package
- all the currently suppressed reports on privacy and costs are publicly released

- the public consultation process is complete and the results publicly available, and
- the design specifications are complete and publicly available.

No doubt the Government will seek to scare opponents into supporting the legislation, on the basis that its own mismanagement of the tendering process could expose taxpayers to millions of dollars in liabilities for contract variation or cancellation, should details of the scheme now be changed by Parliament. We urge you to resist such pressure - neither Parliament nor the Australian people should be blackmailed into supporting this scheme.

We therefore also urge the Committee to recommend to the Government that all tendering or awarding of contracts by the Government cease, until such time as the design specifications are complete, and *all* related legislation has been passed by Parliament.