Australia's proposed ID Card: Still quacking like a duck

Graham Greenleaf,
Professor of Law, UNSW
Co-Director, Cyberspace Law & Policy Centre
11 November 2006
Submitted for publication in *Computer Law & Security Report*

Introduction – the second coming?

Almost twenty years ago, Australia rejected the attempts of the Hawke Labor Government to introduce a national ID card system, the 'Australia Card'. Its ignominious defeat (Greenleaf, 1988) ensured that Australian politicians ever since then have hastened to assure the public that any new surveillance scheme they are proposing to introduce is 'not another Australia Card'.

Australia in 2006 is debating the proposed introduction of what the conservative Howard government calls a 'health and social services Access Card'. It lacks a catchy name this time, though the Minister for Human Services has floated 'the People's Card'. Whatever it is called, the government has insisted since its announcement in May 2006 that it is not a national ID card. Prime Minister Howard insists that Cabinet debated that alternative and rejected it. Minister for Human Services, Joe Hockey states that new legislation will state it is 'not a national identity card' (Hockey 2006). The 'Consumer and Privacy Taskforce' ('Taskforce'), the government-appointed watchdog of the proposal, in its first Report (Taskforce 2006b) states that:

> 'Since the idea of having a national identity card has been clearly ruled out by the Government and according to public opinion polls is not supported by the Australian public either, it becomes important to ensure that the health and social services Access Card does not become, now or in the future, a national identity card by any other name.'

The Australian situation therefore contrasts with the United Kingdom, where it is accepted that an unprecedented introduction of an ID card and system supporting it is underway.

Is a new national ID card proposed?
It is possible to argue at length about what constellation of factors constitutes a 'national ID card'. The answer in a federation like Australia may differ somewhat from a country like the UK. The Taskforce, despite its rhetoric above, has not been very useful in clarifying exactly what would constitute the 'national identity card' we are all agreed that we wish to avoid. In both its Discussion Paper (Taskforce, 2006a) and more recent Report (Taskforce 2006b) it put forward a straw man:

> "A national identity card system would include the aspects of its being compulsory, producible on demand by certain authorities, a requirement for people to carry it at all times, its linkage with a unique identifying number and the fact that it is the sole form of identification recognised by Government authorities."

Few ID card systems anywhere in the world are this draconian. On these criteria, the Australia Card would not have been a national ID card, a proposition which few Australians would accept. Why do all government authorities have to recognise only one ID document? Is what the private sector requires for identification irrelevant? Why does there have to be 'a requirement for people to carry it at all times'? For example, Hong Kong obviously has an ID card (Greenleaf 2006a), but some government agencies will accept other ID documents for some purposes; it is not required that the ID card be carried at all times (though the government does have powers to require this); and the Privacy Commissioner's Code dealing with the ID card attempts to limit the uses the private sector makes of it. The constellation of factors making up what can reasonably be called a 'national ID system' is clearly complex. In this article I'm not going to attempt to propose some trans-national set of necessary or sufficient conditions.

However, it is clear that 20 years ago Australians saw the 'Australia Card' proposal as an ID Card (and ID system), and rejected it as unacceptable (Greenleaf 1988). It is therefore informative to compare the current proposal with that of 20 years ago. No matter what the government prefers to call it, if it has a sufficient 'family resemblance' to the one 'ID card' and ID system that we knew – and most people loathed - then it is one. The purpose of this paper is principally to explore that issue: if the 'Australia Card' was a national ID card scheme, then is the 2006 'Access Card' proposal also one according to the same criteria?

Such a comparison is also a useful way to explain what is proposed in the 'Access Card' proposals, by providing a comparison with what was technically feasible 20 years ago, compared with the significant changes in the new smart-card based proposal.

Basis of comparison

Although over six months have elapsed since the 'Access Card' proposals were announced, the Australian government has still released very few details of its proposals. In my opinion it is intentionally releasing as little as possible about its plans, so as to present as small a target as possible to potential critics. There are only a few pages of details in the federal Budget (9 May 2006) documents despite inclusion of $1B to fund the Card scheme, and only a page or so from the Government's announcement of the proposal a fortnight before (see Human Services Home page). A month after the Budget, the Government finally released a heavily edited version of the KPMG 'Business Case' for the scheme (KPMG 2006). The Privacy Impact Assessment (PIA) carried out in conjunction with the KPMG study has not been released despite numerous requests. The Taskforce members are Professor Alan Fels, former competition regulator, a former NSW Privacy Commissioner (Chris Puplick) and a former deputy defence ombudsman (John Wood). The Taskforce has no statutory basis or detailed terms of reference, and must report to the Minister (not the public). The Taskforce's Discussion Paper (2006a) and first Report (2006b), the Government's response (Australian Government 2006a), and the Minister's Press Club speech (Hockey 2006), add few significant details to what was known or assumed from the KPMG report, but often confirm matters assumed. In a few significant cases they contradict them. As a result, my analysis of six months ago remains largely unchanged (Greenleaf, 2006b). This comparison below is therefore necessarily tentative, but is made on the best information available.

Details of the 1986-87 Australia Card proposal are taken principally from the most detailed published analysis of the legislative and technical structure of that proposal (Greenleaf 1987), supplemented by other sources (Caslon Analytics 2005). Other studies detail the dangers and fate of the Australia Card (Clarke 1988, Greenleaf 1988). For ease of reading the Australia Card will sometimes be referred to in the present tense, as if it currently existed, and as if its enabling legislation had been passed. References to clauses in the Tables following are to the *Australia Card Bill 1986* (not enacted).

A more important comparison: Dangers to privacy

Irrespective of questions of labeling as an ID card or ID system, the more important questions are 'what dangers to privacy does this smartcard-based scheme pose? – and how do they compare with the dangers of the Australia Card?' In the final column of the Tables below, I have made a subjective assessment of whether the dangers to privacy of the new proposal are 'worse', 'less' or (the) 'same' as the Australia Card. Readers are invited to decide whether their assessment differs from mine. Where this assessment depends on details yet to be revealed, 'undisclosed' is indicated. I should stress that an assessment of privacy dangers is not a cost/benefit analysis: there is always a level of risks or dangers to privacy which may be justified by other social benefits to be obtained. This analysis is simply a comparison of risks between the current and earlier proposals.

A universal, compulsory ID card

The Access Card will be compulsory and near-universal for adults in exactly the same way as was the Australia Card: it is not as a rational and practical matter possible to do without a Medicare Card in Australia in 2006, just as it was not rational or practical in 1987 to pay the top marginal rate of tax on all transactions and do without a Medicare Card. In both cases the supposed voluntary nature of Card possession can better be described as 'pseudo-voluntary'. The Taskforce (2006b) "recognises that, at

some stage, almost every Australian is likely to need an Access Card and as such to become a person registered in the Secure Customer Registration Service" (the back-end database).

Children were to have an Australia Card from birth, whereas now their details will be entered on their parent(s)' cards. The privacy dangers may be somewhat less than each child having their own card.

Neither card is required to be carried at all times, but production is required by law for some transactions. For the Access Card production requirements are to be limited to 'health and social security purposes' (Australian Government 2006), which will cover three federal government agencies, may include some State agencies, and may include production to private parties such as doctors. For the Australia Card production was to be required only to three agencies also (though the Taxation Office was one of them), and a different range of private sector bodies.

A compulsory uses of children's details beyond anything envisaged for the Australia Card, namely 'bundying in' to pre-school, has been floated by a government Minister (ABC Radio AM, Brough interview, 2 June 2006 and Stafford, 2006), but seems to be contradicted by later statements that the Card can only be demanded for health and social security purposes.

In order to obtain a card a person must produce other identity documents to a government agency and prove their identity in order to be registered. The exact proof of identity (POI) requirements are unspecified. The basis on which an Australia Card could be confiscated by authorities was uncertain, though protection against confiscation when *voluntarily* produced to anyone else was guaranteed by law. It is proposed that the Access Card will be the property of the card-subject (Taskforce 2006b, Recommendation 8, accepted by Australian Government 2006). Exactly what a property right in an ID card will achieve is uncertain and has been described as a *reductio ad absurdum* of 'privacy as property' (Greenleaf 2006c), but it should provide some legal protection against an ID card being retained or confiscated by anyone, because of risk of this constituting an offence larceny or the basis of an action such as for detinue (but with what damages?). Neither scheme guarantees against the validity of a Card being cancelled, which would seem to be a more important consideration.

In summary, there seems little to distinguish the two schemes in terms of compulsion, coverage, and carriage of the Card, except perhaps in relation to children.

Table 1 – Compulsion and coverage

Point of comparison	***'Australia Card' proposal 1986-87***	***Access Card proposal 2006-***	***Privacy dangers***
Adult coverage	Every adult	Every Medicare recipient, plus others	Same
Children	Card from birth	No card until 18 Listed on parents' cards	Less
Compulsory?	'Pseudo-voluntary' – top marginal rate of tax payable unless presented for transactions; no access to social security or health insurance benefits	'Pseudo-voluntrary' – no Medicare benefits or other government benefits unless produced	Same
Carriage?	No legal compulsion (cl 8) – except when required to produce (very often)	No legal compulsion – except when required to produce (very often)	Same
Confiscation?	• Illegal to confiscate if produced voluntarily (cl 170(1)) • Uncertain - confiscation 'for good cause' on compulsory production	Ownership of card proposed; Uncertain - specific protections against confiscation	
Registration	Attend government office to	Attend government office to prove	Same

requirements	prove identity	identity 4 ID documents necessary, with copies to be retained online in SCRS	
Preventing issue of fraudulent IDs	Registration requirements	Registration requirements and comparison of photograph templates (Case Study – Fraud; Fact Sheet - Technology); documents presented to be checked against new Document Verification Service (DVS)	Same
Re-issue	[uncertain]	7 years; new photo required	Same
Lost/stolen cards	[uncertain]	[uncertain] Fee to re-issue	Same

The Card, chip and card readers

The Australia Card was primitive compared with its 21st century successor. It did not have any storage of data not visible on the card face, whereas the 2006 smart card, the Access Card, will have a chip storage capacity of at least 64KB. The Australia Card had a magnetic stripe to record the ID number and perhaps a tiny amount of other text, to make it machine-readable.

The data on the face of the Access Card is much the same for the Australia card: name; photograph (both on the card front); a unique, universal, compulsory national ID number; signature and card expiry date (on the card back). These card face features are, in my view, enough to make them both 'national ID cards': a near-universal relatively high integrity photo-ID card of 'biometric quality', with signature and unique number. Australia does not at present have any universal photo-ID, or universal ID number. Driver's licences are State-based and not universal.

The compulsory data on the chip in the 2006 Access Card will include all the card face data, but will also include more extensive and sensitive data. This will include an up-to-date address, date of birth, details of children and other dependants, and the 'legal name' of any person whose alias appears on the card face (Hockey, 2006). On current policy, 'permanent concession status', indicating age, will only be included on the chip, not the card face, though this is not still under debate (Taskforce 2006b). The Australia Card had no capacity to contain anything but the card face data, so all of this compulsory information on the chip goes beyond what the Australia Card attempted. All of these additional items are potentially sensitive personal information. It appears that this compulsory data on the chip will be included in what Minister Hockey calls 'the locked zone' (Hockey 2006), which may refer to encryption of data but no details are given.

The Access Card number will be a unique personal ID number for each and every Australian adult. This is unprecedented in Australian history. The current Medicare number, the most extensive current numbering system, is not unique and is shared between family members on Medicare cards (though there are unique individual numbers in the Medicare database: Taskforce 2006b). The Access Card number may be created by extending the Medicare number to make it unique (KPMG), and may therefore also indirectly indicate a marital relationship. The number will be on the card back, the chip and the back-end (SCRS) database (Taskforce 2006b). The Taskforce, after lengthy discussion, recommended against any visible inclusion of the ID number on the Card, or alternatively that its visible inclusion by optional (Taskforce 2006b, R18), but the Government rejected this (Australian Government 2006). However, the head of the Taskforce has stated that the Minister has said he will 'think about' the option of a new ID number being assigned whenever a Card is lost (ABC Radio National).

Inclusion of a signature on the card will also be unprecedented in Australia. There is no single document at present that everyone must sign. A digitised copy of the signature will be on the Card back, and on the back-end (SCRS) database, but is not mentioned by KPMG or the Taskforce as being included in the chip. This is not a 'digital signature', which is a number used for purposes of

encryption and decryption. The Taskforce recommended that the signature should not be included on the Card or database, stating that it is 'not aware of any robust argument which has been advanced for its inclusion' (Taskforce 2006b, R15), but the Government rejected this, simply alleging that it 'provides greater utility and security for the cardholder' (Australian Government 2006) and will 'make it easier to cross-check signatures' on paper forms' (Hockey 2006).

The Access Card chip may also contain extensive optional data including medical information, but the range of potential optional data has not been defined yet. Minister Hockey likens the Access Card to a 'mini-iPod, where you can download limited amounts of information on to the microchip and carry it around in your wallet or purse' (Hockey 2006). He refers to a 'Customer Controlled' part of the chip, apparently referring to PIN-number access, where 'owners'

> 'will be able to customise your card with the addition of personal information like emergency contact details, next-of-kin, allergies, organ donor status and health alerts. You will be able to add other information that you wish to include.'

The potential storage of any information, whether compulsory or voluntary, depends on the chip size. KPMG (2006, p37) proposed a 64KB chip 'subject to detailed design information', but claims that the 'initial functionality' will only need 22-23KB. 'This could be scaled up to 128KB if desired…', it said. The Taskforce (2006b) considers that the current proposed uses will only use 75% of a 64KB chip. The government has not yet made any commitment as to whether chip size will be 64KB or larger (Australian Government 2006).

An extraordinary inclusion is that emergency payments ('smart benefits') 'would go direct to the smart card' (KPMG 2006, p67 and p45), which means either that the card will have to have 'electronic purse' capacity or that it can be used at an ATM to obtain a cash payment to the cardholder. The government is committed to go ahead with this function (Australian Government 2006), but the Taskforce says it has no information as to how this would work (Taskforce 2006b). In relation to a more general e-purse capacity, the Taskforce says it understands that the Minister 'has clearly ruled out this proposed use for the Access Card in its current iteration', but notes that an e-purse function has 'wide support in a number of quarters' (Taskforce 2006b), presumably the financial sector.

It is assumed by the Taskforce (2006b) that the Access Card smart card requires contact with a card reader for the chip to be read, though KPMG does not specify and the Taskforce is not sure. The dangers to privacy of unauthorized access to data on the Access Card, or use of the card itself, are obviously greater than with the Australia Card, whether the Access Card is contact-required or contact-less. A contact-less card would greatly increase privacy dangers.

The role that both encryption and PIN access will play in controlling access to data contained on different zones on the chip is still quite obscure. When the role of data encryption is clarified, it will also be necessary to define who will be entitled to have 'authorised' card readers (ie those which have the necessary decryption capacity), and what penalties will apply to anyone who attempts to decrypt encrypted card data without authority. It seems a reasonable assumption that the compulsory data on the Card will be protected by encryption, so that it can only be read by 'authorised' card readers. Whether the card-holder will also need to provide a PIN once they present their Card to someone with an authorised card reader is unknown. These are fundamental questions about any smart card system, but they are not addressed in the publicly-released parts of the KPMG report, nor in the Taskforce's publications.

According to KPMG, for security purposes the data on the chip will be segmented into 'Public' (no PIN needed) or 'Closed' (PIN access required) zones, but apparently only into those two zones. Minister Hockey may have renamed the 'Public' zone as the 'locked' zone, and the 'closed' zone as the 'Customer Controlled' zone (Hockey 2006), but it is uncertain whether he is referring to a different and perhaps overlapping distinction. He refers to anyone being able to use the Access Card to access government services online by the purchase of an A$25 card reader, so this is obviously not a reference to an authorised card reader. There are privacy dangers involved in allowing online

transactions ostensibly by a person to take place on the basis of possession of their Card and a PIN number, and these are dangers which may not have had equivalents with the Australia Card.

At least some optional data placed on the chip will be protected by a PIN, and it seems reasonable to assume that it can otherwise be read by any card reader. It seems that other optional data can be placed on the chip but without any requirement of PIN access. However, this is speculation. According to KPMG card-holder has to choose whether to put their (optional) medical information etc into the public or closed zone (KPMG p45). If in the public zone, any ambulance or hospital with a reader can access the data whether or not the patient is able to tell them his PIN. But so can anyone else with a card reader. However, if they protect their privacy against access by non-medical personnel by putting their personal data into the closed zone, emergency medical staff will not be able to access it unless they are conscious and can advise of their PIN. This dilemma is inherent in a card with both medical and non-medical functions.

Other than for the fact that both cards will have much the same visible data on the card face, every aspect of the stored content of the card, its accessibility and security, presents far greater dangers than did the Australia Card.

Table 2 - Card content

Point of comparison	***'Australia Card' proposal 1986-87***	***Access Card proposal 2006-***	***Privacy dangers***
ID number	Unique number for each person on card face and central register	Unique number for each adult, on card face (back); on chip; and on central register	Same
Card face data	• ID number; name; photograph; signature; card expiry date • DOB for children only	• name; photograph (on front); ID number; signature; card expiry date (on back) • possibly concession data	Same
Card storage capacity	• Miniscule – magnetic strip only (if implemented) • no chip - not a smart card	• magnetic strip • At least 64KB on chip • Must support all Table 4 uses	Worse
Data on magnetic strip	• Might contain card face text content (not photo or signature) (cl17(7))	• ID number; name	Same
Data on chip (compulsory)	• None - no chip	*Compulsory data: (KPMG p37)* • all card face data above except signature, plus the following • address; (to be kept up-to-date: Case Study – Emergency Relief) • date of birth; • details of children & other dependants (identifier, names and DOB) • concession and safety net status flags and expiry dates • emergency payments (KPMG p67) – operation uncertain	Worse
Data on chip (optional)	None – no chip	*Optional data: (KPMG p37and case studies)* • emergency contact details, • 'allergies, health alerts, chronic illnesses, immunisation information and organ donor status'	Worse

		• details of carer; or of carer status re other identified person • other optional data, no limits	
Data related to security	None	• encrypted PIN number (KPMG) • 'Secret Questions and Answers' for use in remote communities (KPMG p21) • 'digital certificate' (KPMG p21)	Worse
Contact required to read chip	Contact required for magnetic strip; otherwise data only able to be viewed	• [Assumed] contact required for card reader	Same
Segmentation and encryption of card data & access to it	N/A	• 'Public' or 'closed' (PIN access) zones only; • DVA, HIC and DHS readers only write-enabled readers • Encryption of data unknown	Worse

The national registration database and access to it

As with all ID systems, the card is only the visible part. The back-end computer systems, particularly including any central register, the card-readers, and the communications network to enable card-readers, central registry, and other computers in the network to communicate, are each just as important. KPMG has proposed that there may be private ownership of both the communications network and the card readers for the Access Card (KPMG p41), and Australian financial institutions are reported to be enthusiastically promoting the possibility of their running a network that cold support both financial smart cards (which have not yet got off the ground in Australia) and the Access Card. The Australia Card network was to remain in government hands. The privacy dangers of a partly privatised national ID system would seem to be somewhat greater than one in government hands. The Health Insurance Commission (HIC) was to run the Australia Card system. Medicare, successor to the HIC, is also within the Department of Human Services, whose 'Access Card Office' will run the Access Card system.

Card reader access to the chip content Questions of availability of card readers did not figure in the Australia Card debates as there was nothing to read on the Australia Card that was not visible on the card face. As discussed earlier, with the Access Card issues of availability of card readers, what they can read, and penalties for misuse, are far more complex and central to the privacy dangers of the system. Most key questions are as yet unanswered. However, it is clear that many thousands of people across Australia (perhaps hundreds of thousands) will have authorised access to card readers, including employees in any offices of the agencies of Human Services (DHS), including social security and health insurance (HIC), and Veteran's Affairs (DVA), and workers in health and allied professions including in every doctor's surgery. Unless all providers of medical and related services have card readers, the option to add this data to the card will be pointless. If every person who buys a A$25 card reader can potentially access some information on cards, another layer of complexity is introduced. The possibility of card readers being available in pre-schools, ATMs etc increases complexity further. The privacy risks dwarf anything contemplated in relation to the Australia Card.

Central register content Both ID systems depend on a central register or 'back end database': the Australia Card Register and the Access Card's 'Secure Customer Registration Service' (SCRS). Both registers were to contain names ('legal' and aliases), addresses (current and recent), ID numbers, digitised photos and digitised signatures. The Australia Card register was to contain little more than this, though that collection of data would in itself be unprecedented, as it still is in 2006 with the Access Card. In neither system would data from different agencies be aggregated. In both cases the function of the central register is more in the nature of a switchboard, enabling identity details to be initially verified so as to enable a Card to be issued, and then to keep those identity details, and information about Card status, up-to-date with the assistance of the participating agencies.

However, the SCRS is far more than the Australia Card register was ever proposed to be, in relation to three aspects of what it will store: (i) sensitive personal information, both optional data and compulsory data about concessions; (ii) proof of identity (POI) data; and (iii) photo templates as well as the photos themselves.

The SCRS was proposed by KPMG to contain a copy of all the emergency contact, medical and other optional information (see Table 2) that a person chooses to store on their ID card (KPMG p42). This is ostensibly 'to allow lost cards to be replaced', presumably without need for re-capture of such data. However, the register will also be an attractive source of otherwise unobtainable intimate data, attractive to police, security and other investigators. KPMG nevertheless makes the extraordinary claim that the SCRS 'will not contain any sensitive personal information' (p39). The Minister now suggests that this data may be backed up on 'a separate database chosen by the individual' (Hockey 2006), but without suggesting whether this is the SCRS or something else.

The SCRS will also contain details of a person's concession status for DVA, age pension and seniors (permanent concessions) and for MRS, PBS, RPBS and safety net eligibility (temporary concessions) (KPMG p42). This concession information can lead to very sensitive inferences about a person and their conduct, and it is again extraordinary that KPMG would not regard this as 'sensitive personal information'.

One of the potentially most dangerous KPMG recommendations is that the SCRS will also contain digitised copies of all POI documents used by the cardholder to register (KPMG p49), such as passport, birth certificate and driver's licence. These documents will contain sensitive personal information not otherwise found on SCRS, and not found together in systematic form anywhere else, so they increase the privacy dangers substantially. An example is mother's maiden name, found on a birth certificate, and commonly used for password reminder and other purposes. Availability in a central register like this is a major security risk to individuals. The Taskforce recommended that POI documents should not be 'scanned copied or kept once verified' (Taskforce 2006b, R20). The Government's response was that it 'partially supports' this, meaning they 'will explore relevant legislation and business procedures with a view to implementing this recommendation'. In other words 'we will tell you later which data we would like to keep forever, but we might not keep everything'. So the extent of privacy threat posed by this 'POI database' remains uncertain.

The SCRS will also contain a facial biometric template generated from the cardholder's photograph (KPMG p21), which is to be 'capable of one to many matching' (KPMG p16). It is also proposed that SRCS will contain a copy of the digital photo of each person, in addition to the template, of sufficient quality to generate such templates. The Taskforce (2006b) states that the addition to SCRS of what it calls 'the first national photographic database of (virtually) all adult Australians' 'changes its nature qualitatively and fundamentally'. It points out that while a number of European nations have national photographic databases,

> 'with the exception of The Netherlands and Belgium, these databases appear not to contain biometric quality photographs and so cannot be used in the same way as is proposed for Austrlia'.

The SCRS will use this capacity in order to try to identify individuals who are applicants for multiple cards (KPMG p49), the potential other uses must be considered. SCRS will be the most comprehensive photo repository of Australians, by some orders of magnitude, and the photos will be 'biometric quality' in addition. Given that the photos are explicitly 'capable of one to many matching', this will be an enormous attraction to Police, national security and other investigators who wish to try to identify a person of whom they have a photograph or even a set of facial parameters approximating a template. The Victorian Privacy Commissioner has warned of the dangers of the joint Australian governments (COAG) development of a national framework for Closed Circuit TV (CCTV) (Chadwick 2006). The potential interconnection of a national government CCTV framework and a comprehensive national photo database with one-to-many matching capability should not be ignored. DHS officers responsible for the ID card have admitted it is under consideration (Senate Estimates Committee, 25/5/06, question by Senator Stott-Despoya to Mr Bradford). The Taskforce

notes that such use is 'certainly possible' and notes other potential uses such as racial profiling and medical diagnostics (Taskforce 2006b).

Network access to the central register and other computers There is going to be a very high level of network traffic in the Access Card system. Every time a person visits a GP or pharmacist their card will be used to check with the SCRS their status in relation to temporary concessions (KPMG p42). Each participating agency will advise SCRS whenever a concession threshold is reached (KPMG p43), so the SCRS will also have to contain a flag about pension status. Wherever a person notifies a change of address, participating agencies will be notified by SCRS (KPMG p65). The Australia Card Register was to play a similar 'switchboard' function, except inclusion of concession data was not proposed.

Whereas the Australia Card register was to be linked to a proposed new national Births Deaths & Marriages system (not subsequently implemented), linkage between the SCRS and the Document Verification System (DVS) to be operated by the Commonwealth Attorney-General's Department (KPMG p50) will play a very similar role.

Despite the government's rhetoric of consumer service delivery, the one service they refuse to deliver is to enable online checking of whether a cardholder has reached the Medicare safety net threshold. Although it is very difficult for the most disadvantaged members of the community to calculate this, the government has excluded this capacity because it might cause over-servicing (KPMG p43).

This level of networked access and surveillance in relation to the use by benefit agencies is much the same as what was proposed in the Australia Card scheme. Access from doctor's offices and the like may well be greater, but may not have any significant effect on privacy. However, the danger of privacy-infringing access – both authorised and unauthorised – to all three of the additional forms of data discussed above is likely to be far greater than was the case with the Australia Card Register.

To sum up, on most criteria relating to the national registration database and access to it, the Access Card proposal presents greater dangers to privacy than the Australia Card, though the underlying architecture is in many respects the same.

Table 3 – The central computer system, card readers and networking

Point of comparison	***'Australia Card' proposal 1986-87***	***Access Card proposal 2006-***	***Privacy dangers***
System operator	Health Insurance Commission ('the Authority')	Department of Human Services ('Access Card Office')	Same
Possession of card readers to access chip	Uncertain who would possess; relevant to magnetic strip only; not significant	• DVA, DHS, HIC – 'full read and update functionality' (KPMG p40) • All doctors, pharmacies – networked readers (KPMG p40) • Ambulances, hospitals, etc needing health data - non-networked readers (KPMG p40) • Financial institutions, via ATM/EFTPOS terminals (Case Study – Emergencies) • Supermarkets, in EFTPOS registers (Hockey, media interview) • [uncertain] Pre-schools, so infants can 'bundy-in' • Self-service kiosks (KPMG p46)	Worse

Central computer system and content	'Australia Card Register' (cl 23) including • name, ID number, nicknames, alias • DOB and DOD • citizenship status • digitised signature and photo (cl 25) • current address (as changed) and for last two years • gender (and re-assignment) • link to BD & M register (details of docs produced to establish identity: Sched 1)	'Secure Customer Registration Service' (SCRS), including • all compulsory data on chip • digitised signature • photo template • all optional data on chip [KPMG p40] • Concession status (KPMG p42) • copies of all POI documents (KPMG, p39, p56) • [assume] relevant benefit agencies (to inform change of address etc)	Worse
Linked systems for POI checks	• National BD&M Register on same computer (cl 71) with remote terminal access (cl 75) • Authority can access BD&M Register to maintain Australia Card Register	• Links to A-Gs Document Verification System (DVS)	
Linked computer systems / access to Register	• ATO, DSS & HIC only to have online access; online access allowed (cl 59) but oversight body could limit terminal numbers (cl 65)• DIMEA to get address data on prohibited non-citizens (cl 180) • Updating data to flow continuously to (but not from) Register from 6 other agencies (cl 14) • links to BD&M source documents • Register can require ATO, DSS & HIC to inform of changes re clients (cl 29), and can be required to inform them (cl 67); they can then inform Police (cl 174) • No other access via card readers known (any readers could only read magnetic strip)	• [unknown] number of linked systems (network configuration deleted from KPMG 2006) • SCRS will notify all DHS and DVA agencies of address changes etc (KPMG p46) • Agencies will advise SCRS when concession thresholds reached. • SCRS link to Document Verification Service (DVS) to validate POI documents (KPMG p50) • Readers of doctors, pharmacies 'accessing real-time concessional status' (KPMG 41)	Worse
Ownership of network and readers	Government	• May be private ownership of network and readers (KPMG p41)	Worse

Few restrictions on uses of the Card and ID number

It is proposed that use of the Access Card will only be required in relation to transactions involving claims for health or social security or ancillary benefits. Legislation will prohibit the Card being demanded in other circumstances (Australian Government 2006). However, the required uses of any ID card and number are only part of what must be considered in assessing its dangers and whether it amounts to a 'national ID card' system. Other likely current uses, and the possibility of future required uses, must both also be considered. As the Taskforce puts it, 'in between the poles of express usage and express prohibition lies a grey zone' (Taskforce 2006b).

First, whether non-required uses of either the card or number are prohibited, allowed or encouraged, must be considered. Only if other uses are prohibited can the claimed purpose of an ID system be accepted as its real purpose. For example, any uses of Australia's Tax File Number (TFN), other than those required by law, are prohibited. Second, the technical and legal impediments to later expansion of required uses must also be considered as major factors, because the 'function creep' of ID systems is one of their most common characteristics.

Pseudo-voluntary uses of the Card The Australia Card was characterized by quite limited required uses within the Commonwealth public sector (no broader than proposed for the Access Card), and production was required in a range of finance-related transactions. It would have been illegal to demand production of the card outside these contexts. Similar requirements for production and prohibitions on demands for production are proposed for the Access Card. Much of the opposition to the Australia Card resulted from the well-founded perception that, despite these ostensible limits, it was intended that the Card would in fact be presented routinely as a photo ID card, and that organizations would come to expect this: 'pseudo-voluntary' production (Greenleaf, 1987, Clarke 1988). Furthermore, the use of the Australia Card ID number (whether voluntary or required) was not proposed to be restricted, provided it was not accompanied by a demand for the card for verification.

The Access Card proposal, on what is known at present, is at least equally dangerous. The government has not proposed to make any non-required uses of either the card or number illegal. In fact, it explicitly states that the card may be used as POI to other Commonwealth agencies and State agencies (KPMG p45), and in the private sector. Uses are envisaged "such as accessing a transport concession, joining a registered club, applying for a passport, or obtaining airline tickets" (KPMG p17). Elsewhere they comment that "there is no reason why the card could not be used by a consumer as for POI purposes to access services from other Commonwealth agencies in the initial roll-out of the card" (KPMG p45). The Minister states (Hockey 2006) that

> 'The card may be used by you, at your choosing, as an identification tool in the broader community … Our proposed legislation will prevent the card being required by a bank or other organisation as the only allowable form of identification. People may, however, choose to use the Access Card to assist in Proof of Identity.'

This is exactly the same as for the Australia Card. Banks and other organisations will still be able to set their own POI requirements so that production of an Access Card is so overwhelmingly more convenient than any other form of identification that it will become a *de facto* universal ID card, provided they keep open the theoretical possibility that some much more inconvenient combination of identifiers can also be used. So long as they can set their own rules about this, it can best be described as 'pseudo-voluntary' production, as it was with the Australia Card. This applies equally to the Commonwealth public sectors, State and Territory public sectors and the private sector. It is very unlikely that the 'collection principles' of an information privacy laws which apply to those sectors would prevent such 'pseudo-voluntary' production of Access Cards as ID. The result is likely to be a national ID card in practice.

Uses of the number In contrast, the collection and use of the Access Card ID number by private sector organizations will be limited by National Privacy Principle 7 in the *Privacy Act 1988* (Cth), which restricts the use of Commonwealth government identifiers by private sector bodies. Although the *Privacy Act* also has many exceptions (eg small businesses, employment uses), this will probably stop the Access Card ID number becoming a universal identifier in the private sector. The collection and use of the ID number would not be similarly restricted for Commonwealth agencies or State and Territory agencies, unless it could be argued that its collection was unnecessary or unduly intrusive under the collection principles in relevant laws. This is an argument which is plausible but as yet untested. Many such agencies will also often be able to rely on explicit powers to demand information which may override any limitations in collection principles. Australia's information privacy laws are more extensive than they were at the time of the Australia Card (when no such enforceable laws existed or were proposed), so in relation to the ID number becoming a universal numbering system within Australia, the extent of dangers are less in the private sector and depend on

untested protections in the public sectors. In addition, there is nothing to stop any Australian government from changing existing laws and requiring or allowing more use of the ID number.

In summary, usage of the Access Card as a general purpose national ID card and number is even more likely than it was with the Australia Card scheme. In relation to the ID number it is difficult to make an assessment in relation to the public sectors, but likely that the dangers are lower in relation to the private sector..

Table 4 – Uses of the Card and ID number by various sectors

Point of comparison	***'Australia Card' proposal 1986-87***	***Access Card proposal 2006-***	***Privacy dangers***
Technical restriction on expanded uses	• No card storage capacity; more data could be added to card face on re-issue	[Uncertain] Depends on size of chip; Chip size can be expanded on card re-issue	Worse
Legal restrictions on expanded uses	• Constitutionally impossible to prevent change by legislation • New requirements to produce Card, or new accesses to Register, required legislation • Australia Card Bill did not allow changes by regulation	• Constitutionally impossible to prevent change by legislation • [Uncertain] Capacity to add uses by regulation or administration unclear; no proposals for legislative restrictions	Worse?
Cth public sector uses of card	Production required to 3 agencies only (ATO, HIC, DSS) for various benefits (cl 51, 52, 54)	• Production required to Medicare and all DHS agencies and DVA, for 17 benefits	Worse
Cth public sector uses of ID number	• ID card Bill did not restrict; Privacy Bill may have done so	• Restriction by IPPs as 'excessive collection', untested as yet	Same
State/local govt. uses of card	• Wide use of number expected • National Births Deaths & Marriages register to be on same computer as Aust. Card Register and run by HIC (cl 4)	• Wide use encouraged, particularly by State agencies requiring ID checks (PM) • To be used as 'a general proof of identification' (Case Study – Pensioner; 'Access Card at a Glance')	Worse
Health sector uses	• Production required to hospitals (cl 53)	• Required to doctors and pharmacies • All health sector organizations must have access to chip for Medicare and optional health information	Worse
Financial sector uses	Production required to 10 types of financial institutions (cl 40-48) and to employers (cl49-50) for reporting to ATO only	• Chip readable by ATM/EFTPOS terminals (when built) 'to access government emergency relief cash payments' (Case Study – Emergencies)	Can not compare
Other private sector uses of card	• Otherwise illegal to require card (cl 167(1)) • But 'Pseudo-voluntary' production allowed – anyone can 'request' Card; holder has right to use cards as ID (cl 8(3)	• Card can only be required re health social security and related benefits • To be used as 'a general proof of identification' • Anyone many request Card	Same
Private sector uses of ID number	• Not illegal to require, record and use number – only to require verification from card • Otherwise illegal to use	• NPP 7 limits use of ID number – unless ID legislation over-rides	Better

	numbers recorded when production required (s170(10))		

Technical and legal capacity for expanded uses The Australia Card system's technical capacity to expand uses it could support depended on the expandable capacity of the central register, not that of the Card itself. With a smart card, the technical capacity to expand the required or encouraged uses depends on the storage capacity of the card as much as the expandability of the back-end capacity. As explained, the additional capacity of the chip (beyond the original list of required functions) is not yet clear, but even on the minimum size of 64KB apparently under contemplation there seems to be significant capacity for expansion of functions.

While it is not possible to prevent future Parliaments changing the uses that can be made of an ID card or system, or the data that can be added to a card, the *Australia Card Bill* did require new legislation before the data on the card could be changed, before the card could be required to be produced in new situations, or new accesses allowed to the register. Although the Australian government has decided to legislate to legitimate the new ID system, it does not make any commitment that the legislation will control these matters (Australian government 2006). The Taskforce suggested that they should be covered, though it did not make a formal recommendation to this effect (2006b).

The card-holder's rights

The card-holder's rights to access and correct their own information seem much the same for both the Access Card and the Australia Card, though it is possible that the privacy legislation to accompany the Australia Card might not have been even as strong as the *Privacy Act 1988*. It will probably be easier for users to access and change their details on the 2006 card, but this is offset by the fact that there is more to access and to be concerned about its accuracy. There may be some additional fraud prevention features, but the opportunities for fraud are also correspondingly greater.

However, until more details are available of the legislation to control the Access Card, it will the not be possible to assess whether it matches the *Australia Card Bill*'s modest restrictions on expanding content and functions of the card or its use (as discussed above). The overall protection of card-holder's rights will remain uncertain until then.

Table 5: Card-holder's rights and uses

Point of comparison	***'Australia Card' ID card proposal 1986-87***	***Australian national ID card proposal 2006-***	***Privacy dangers***
Data subject access / change card face data	N/A – card face data only, so all data on card visible	• Data on chip not visible • Can access and update some of own details online (Case Study – Family)	Same
Data subject access / change Register data	Privacy Act IPPs 6 & 7	• Privacy Act IPPs 6 & 7 • Change of address feature (below)	Same
Data subject uses	• Change address with any one agency to change with all • No user address change feature but assumed available	• Change address with any one agency to change with all • User can change details online	Same
Prevention of fraudulent use	Card face photo	Card face photo claimed to prevent non-owner from using card (Fact Sheet – Technology)	Same

Conclusions

> "When I see a bird that walks like a duck and swims like a duck and quacks like a duck, I call that bird a duck." - James Whitcomb Riley (1842-1916) (*Wikipedia* entry)

From the preceding analysis, and the comparative Tables, it is clear that almost all the features present in the Australia Card system are present in the Access Card proposal. The resemblances are often striking. Because of the chip, the 2006 smart card also has features that the 'dumb' card of 20 years ago did not have. In most respects the privacy dangers of the new ID system are worse than those of the Australia Card. On the majority of features relevant to privacy that are identified, the privacy dangers are worse or the same as the Australia Card. Only in an insignificant number of features is this system less dangerous to privacy.

'If it walks like a duck and quacks like a duck, it is a duck', as the saying almost goes. Six months into its life, the Access Card still quacks like the Australia Card. That ID card system ended up a dead duck, twenty year ago. Whether this one takes flight remains to be seen.

References

Australian Government (2006) - Australian Government's Response to the Access Card Consumer and Privacy Taskforce's Advice to the Minister for Human Services, November 2006

ABC Radio AM transcript of interview, 2 June 2006, with Minister for Family and Community Services, Mal Brough, proposing Access Card as option for child care centres to be required to use either a swipe card or PIN to be able to receive federal funds; see <http://www.abc.net.au/am/content/2006/s1653586.htm>

ABC Radio National Breakfast, 9 November 2006, transcript of interview of Prof Alan Fels by Fran Kelly

Caslon Analytics (2005) 'Australia Card and Beyond' (2004-05) at <http://www.caslon.com.au/australiacardprofile1.htm>

Clarke (1988) Clarke, Roger 'Just Another Piece of Plastic for your Wallet: The 'Australia Card' Scheme' Computers & Society 18,3 (July 1988); at <http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html>

Graham (1990) - Graham, Peter 'Bureaucratic Politics and Technology: Computers & the Australia Card' (Nathan: Centre for Australian Public Sector Management, Griffith University 1990)

Greenleaf (1987) - Greenleaf, Graham 'The Australia Card: towards a national surveillance system' Law Society Journal (NSW) Vol 25 No9, October 1987; longer version at <http://austlii.edu.au/itlaw/articles/GGozcard.html>

Greenleaf (1988) - Greenleaf, Graham 'Lessons from the Australia Card -- deux ex machina ?" The Computer Law and Security Report, Vol 3 No 6, March/April 1988, pg 6; at <http://austlii.edu.au/itlaw/articles/GGOzcard1-Lessons.html>

Greenleaf (2006a) - G Greenleaf 'Hong Kong's 'smart' ID card – Resources' at http://austlii.edu.au/privacy/HKID/

Greenleaf (2006b) - G Greenleaf 'Quacking like a duck: The national ID Card proposal (2006) compared with the Australia Card (1986-87)', 12 June 2006, available at http://www.cyberlawcentre.org/privacy/id_card/OzCard_comparison.pdf

Greenleaf (2006c) – G Greenleaf 'Australian ID Taskforce Report: A sheep in wolf's clothing' *Privacy Laws & Business International Newsletter*, Issue 85, Nov-Dec 2006

Human Services - Department of Human Services (DHS) - *Office of Access Card* home page <http://www.humanservices.gov.au/access/>

KPMG (2006) - KPMG *Health and Social Services Smart Card Initiative, Vol 1: Business Case (Public Extract)*, released 6 June 2006; at <http://www.humanservices.gov.au/access/>

Taskforce (2006b) - Access Card Consumer and Privacy Taskforce 'Issues and recommendations in relation to architecture questions of the Access Card', 25 September 2006, 68 pgs, available at <URL>

Hockey (2006) - The Hon Joe Hockey MP 'Future Directions for the Access Card: Your Card – Your Security' National Press Club, Canberra, 8 November 2006

Stafford (2006) - Annabel Stafford 'Access card could link to surveillance", *The Age*, 5/6/06

Wikipedia entry for James Whitcomb Riley at <http://en.wikipedia.org/wiki/James_Whitcomb_Riley>