Quacking like a duck: The national ID Card proposal (2006) compared with the Australia Card (1986-87)

Graham Greenleaf,
Co-Director, Cyberspace Law & Policy Centre, Faculty of Law, UNSW
12 June 2006

NOTE – DRAFT ONLY: This is a working draft, being revised – please check with author before citing. The Privacy Impact Assessment (PIA), other privacy advice to the government, and some of the details excessively excised from the KPMG report, are desirable before a full comparison can be made. Revised versions of this paper will be available from the Cyberspace Law & Policy Centre website <http://www.cyberlawcentre.org>.

Introduction – Comparing two card systems

Is a new national ID card proposed?

What the Australian government has labeled as a 'health and social services access card' has many similarities to the rejected 'Australia Card' proposed by the Hawke-Keating Labor government 20 years ago. There are also many points of divergence, often because of capacities provided by the technological changes of the last 20 years.

One of the Government's claims when announcing the card proposal was that Cabinet had rejected proposals for a compulsory national ID Card, and had instead settled on a 'benefit card'. It is possible to argue at length about what constellation of factors constitutes an 'ID card'. However, it is clear that 20 years ago Australians saw the 'Australia Card' proposal as an ID Card, 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' 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 system, then is the 2006 also one according to the same criteria? Is this an Australia Card with a different name?

Basis of comparison

The government is still releasing as few details of its proposals as possible, so as to present as small a target as possible to potential critics. It has not released its own planning documents. 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, plus comments from media conferences, from the Government's announcement of the proposal a fortnight before (see DHS Home page). A month after the Budget, the Government finally released a heavily edited version of the KPMG 'Business Case' for the scheme (6/6/2006). Privacy advice, including the Privacy Impact Assessment (PIA) carried out in conjunction with the KPMG study has not been released. This comparison below is therefore necessarily tentative, and will need to be expanded as more details emerge.

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).

A more important comparison: Dangers to privacy

Irrespective of questions of labeling as an ID card, the more important questions are 'what dangers to privacy does this smartcard pose? – and how do they compare with the dangers of the Australia Card?' In the final column of the Tables, 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. From a privacy perspective, is this proposed system worse than the Australia Card?

A universal, compulsory ID card

The 2006 national ID card will be effectively 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 financial transactions or do without a Medicare Card. Both the 1986 and 2006 cards are 'pseudo-voluntary'.

Children were to have an Australia Card from birth, whereas now their details will be entered on their parent(s)' cards (though children will be individually registered). The privacy dangers may be somewhat less than each child having their own card, though compulsory uses of children's details beyond anything envisaged for the Australia Card, such as 'bundying in' to pre-school, have already been floated by the government[1].

Neither card has to be carried at all times, but production is required by law for some transactions. 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 basis on which an Australia Card could be confiscated by authorities was uncertain, though protection against confiscation when voluntarily produced was guaranteed. No protection at all is proposed for the new Card.

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

Table 1 – Compulsion and coverage

Point of comparison	***'Australia Card' ID card proposal 1986-87***	***Australian national ID 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 (may be required for tracking movement of pre-school children)	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 if could be confiscated 'for good cause' on compulsory production	[uncertain] No legal right to a card yet proposed; [Uncertain] no protections against confiscation proposed	Uncertain
Registration requirements	Attend government office to be photographed, provide signature and prove identity	• Attend government office to be photographed, provide signature and prove identity to extent required (may be reduced for 'known customers': KPMG p30) • 4 ID documents necessary, with copies to be retained online in SCRS	Worse
Preventing	Registration requirements	Registration requirements and	Same

[1] The Minister for Family and Community Services, Mal Brough, has proposed that child care centres be mandated to use either a swipe card or pin number system to be able to receive federal funds, with the so-called access card one option under consideration for use; see ABC Radio AM transcript, 2/6/06 <http://www.abc.net.au/am/content/2006/s1653586.htm>, and Annabel Stafford 'Access card could link to surveillance" , the Age, 5/6/06 <http://www.theage.com.au/news/national/access-card-could-link-to-surveillance/2006/06/04/1149359609088.html>

issue of fraudulent IDs		comparison of photograph templates (Case Study – Fraud; Fact Sheet - Technology); documents presented to be checked against new Document Verification Service (DVS)	
Re-issue	[uncertain]	7 years; new photo required	Same
Lost/stolen cards	[uncertain]	• [uncertain] Stated to be 'unlikely' (Senate Legislation C'tee 25/5/06) • Fee to re-issue; turn-around?	

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 will have an as-yet-unknown chip storage capacity. It has been twice stated by the Minister to be 64MB though this is scarcely believable. KPMG states it will be either 64K or 128K, but the feasibility of this, given the amount of data to be included on the chip (including a photo, electronic purse capacity, dependant details and optional medical data), also calls for independent verification. The Australia Card may have had a magnetic strip to record the ID number and perhaps some other text, to make it machine-readable, and the new card will also have a magnetic strip.

The data on the face of the 2006 card is much the same for the Australia card: a unique, universal, compulsory national ID number; name; photograph; signature and card expiry date[2]. This alone is enough to make them both 'national ID cards': a universal relatively high integrity photo-ID with signature and unique number. On the new card, the unique ID number for each adult will be their current Medicare number 'reformatted where necessary to ensure that it is unique', by inclusion of additional digits (KPMG p41).

The compulsory data on the chip in the 2006 card will include all the card face data, but will also include more extensive and sensitive data, including (as announced to date) an up-to-date address, date of birth, and details of children and other dependants. The Australia Card had no capacity to contain anything but the card face data. The 2006 chip may contain extensive optional data including medical information, but the range of potential optional data has not been limited yet.

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 electronic purse capacity has been confirmed in Senate Estimates hearings[3]. There is also a passing mention of the chip being able to contain a 'digital certificate' (KPMG p21).

I assume the 2006 smart card requires contact with a card reader for the chip to be read (a contact-less card would greatly increase privacy dangers), though KPMG does not specify. The dangers to privacy of unauthorized access to data on the 2006 card, or use of the card itself, are obviously greater than with the Australia Card. For security purposes the data on the chip will be segmented, into 'Public' (no PIN needed) or 'closed' (PIN access) zones, but apparently only into those two zones. A card-holder has to choose whether to put their (optional) medical information etc into the open or closed zone (KPMG p45). If in the open 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 any DHS clerk. 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.

[2] The new one also has 'permanent concession status', indicating age.

[3] Mr Bashford (DHS) states that Centrelink 'will be able to download small amounts of money onto that card which the customer can go and recover from an ATM'; Mr Leeper (DHS) states 'the technology supports its use as an electronic wallet, should government choose to do that' (Senate F&PA Legislation Committee Estimates, 25/5/06, F&PA 79 (proof)).

Table 2 - Card content

Point of comparison	***'Australia Card' ID card proposal 1986-87***	***Australian national ID card proposal 2006***	***Privacy dangers***
ID number	Unique number on card face and central register for each person	Unique number on card face; [assumed] on chip[4]; and on central register for each adult	Same
Card face data	• ID number; name; photograph; signature; card expiry date • DOB for children only	• ID number; name; photograph; signature; card expiry date • plus permanent concession data	Same
Card storage capacity	• Miniscule – magnetic strip only (if implemented) • no chip as not a smart card	• magnetic strip • [Uncertain] 64KB or 128KB[5] on chip • Must be sufficient to support all uses in Table 4	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 from DHS ??? (KPMG p67)	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' • details of carer; or of carer status re other identified person • other optional data, not limited by above (KPMG, p42)	Worse
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

[4] The contents of the chip specified by KPMG (p37) does not include the ID number ('card number'). This appears to be an oversight, as the number would be the most convenient way by which matches between a card and the corresponding SCRS record could be made during any online transactions. The number is also included in the magnetic strip, which would be used for similar purposes, but is expressed to be only a transitional arrangement. If the number is not on the chip, then matches would need to be by cardholder name. Children's ID numbers will be listed on the chip (KPMG p41).

[5] A 64 MB chip was twice announced by the Minister on ABC radio, but this was probably due to the Minister not understanding what he was saying; KPMG (2006, p37) states 64KB '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…'.

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 • [Unknown] Encryption of data	Worse
Suppression of sensitive data	[unknown]	[unknown] Access to address data	Same?

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 (KPMG p41). 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.

Card reader access to the chip content There was nothing on the Australia Card to read that was not visible on the card face. In 2006 the situation is far more complex and the card readers and what they can read far more sophisticated. Questions of availability of card readers did not figure in the Australia Card debates as there was nothing to read, but in 2006 some of the crucial questions (as yet unanswered, perhaps due to censorship of the KPMG report, perhaps due to lack of consideration) are the controls over who will have card readers; who is authorized to use them; and how this will be enforced.

It is clear that many thousands of people across Australia (perhaps hundreds of thousands) will have authorised access to card readers: particularly employees in any DHS, DVA and HIC office, and workers in health and allied professions. But since any card reader will (in theory) be able to read data in the 'public' zone of the chip, the position of card readers in pre-schools, ATMs etc will also require consideration and increase the risks of misuse.

Central register content Both ID systems depend on a central register: the Australia Card Register and the 'Secure Common Registration System' (SCRS). While the Australia Card register contained little more than identification information and current address, the SCRS is also going to contain a copy of all the emergency contact, medical and other 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 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 p 42). 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'.

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. Given that these documents will contain sensitive personal information not otherwise found on SCRS, 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 significant security risk.

The SCRS also contains a facial biometric template generated from the cardholder's photograph (KPMG p21), which is to be 'capable of one to many matching' (KPMG p16). While 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. 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 recently of the dangers of COAG's 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[6].

Network access to the central register and other computers There is going to be a very high level of network traffic in this 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). Wherever a person notifies a change of address, participating agencies will be notified by SCRS (KPMG p65). Whereas the Australia Card register was to be linked to a new national Births Deaths & Marriages system, linkage between the SCRS and the Document Verification System (DVS) (KPMG p50) will play precisely the same 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 is much the same as anything that was proposed in the Australia Card scheme.

On every criterion relating to the national registration database and access to it the 2006 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' ID card proposal 1986-87***	***Australian national ID card proposal 2006-***	***Privacy dangers***
System operator	Health Insurance Commission ('the Authority')	Department of Human Services ('Access Card Office') (Medicare, successor to HIC, is also within DHS)	Same
Possession of card readers to access chip	[uncertain] who would possess; relevant to magnetic strip only	• 'accessed by authorised people' [Budget]; • DVA, DHS, HIC – 'full read and update functionality' (KPMG p40) • All doctors, pharmacies – networked readers (KPMG p40) • Ambulances, hospitals, etc needing health data[7] - non-networked readers (KPMG p40) • Financial institutions, in ATMs and EFTPOS terminals (when built) (Case Study – Emergencies) • Supermarkets, in EFTPOS registers (Hockey, media interview) • [uncertain] Pre-schools, so infants can 'bundy-in' • Self-service kiosks (KPMG p46)	Worse

[6] In response to Senator Stott-Despoja's question "I am wondering if there is any proposal to link the standardized CCTV with the smartcard database. Has that been debated or discussed?", Mr Bashford (DHS) answered "AGIMO are looking at standards around that so we do not have different rail gauges, if you like. We are certainly talking to AGIMO … about that sort of stuff' (Senate F&PA Legislation Committee Estimates, 25/5/06, F&PA 79 (proof))

[7] Unless all providers of medically-related services have card readers, the option to add this data to the card will be pointless.

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) 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	'Secure Common Registration System' (SCRS), including • all compulsory data on chip • signature • photo template • all optional data on chip [KPMG p40] • Concession status (permanent or temporary) (KPMG p42) • copies of all documents used as evidence of identity • Links to A-Gs Document Verification System (DVS) • [assume] relevant benefit agencies (to inform change of address etc)	Worse
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 threshold's 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

The required uses of any ID card and number are only part of the story. Equally important is whether non-required uses of either card or number are prohibited or allowed or encouraged. Only if other uses are prohibited can the ostensible purpose of an ID system be accepted as its real purpose. The technical and legal impediments to expansion of 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 The Australia Card was characterized by quite limited required uses within the Commonwealth public sector (no broader than for the 2006 card), and production required in a range of finance-related transactions. It would have been illegal to demand production of the card outside these contexts. 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. Furthermore, the use of the ID number was not to be restricted, provided it was not accompanied by a demand for the card for verification.

The 2006 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).

While these uses are described as voluntary, it is not clear why there would be any penalty if production of a card was *required* by any of these entities. As the law stands, the collection and use of the ID number by other private sector organizations may be limited by National Privacy Principle 7, which limits the use of government identifiers by others, but the Privacy Act also has many exceptions (eg small businesses, employment uses). The collection and use of the ID number would not be similarly restricted for Commonwealth agencies or State agencies. The government apparently has no proposals at this stage to prevent the card being demanded by other organizations[8], in contrast to the Australia Card Bill which precluded this.

In summary, usage of this card and number as a general purpose national ID card and number is even more likely than it was with the Australia Card scheme.

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

Point of comparison	***'Australia Card' ID card proposal 1986-87***	***Australian national ID 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 • [uncertain] National security uses suggested by Government	Worse
Cth public sector uses of ID number	• ID card Bill did not restrict; Privacy Bill may have done so	• [Uncertain] 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)	Worse
Other private sector uses of card	• Otherwise illegal to use numbers recorded when production required (s170(10)) • 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)	• To be used as 'a general proof of identification' (Case Study – Pensioner; 'Access Card at a Glance') • No restrictions on requiring card production announced; anyone many request Card	Worse

[8] See exchange between Mr Bashford and Mr Leeper (DHS) and Senator Stott-Despoja, Senate F&PA Legislation Committee Estimates, 25/5/06, F&PA 79 (proof), which indicates the government has no proposals as yet.

Private sector uses of ID number	• Not illegal to require, record and use number – only to require verification from card	• NPP 7 limits use of ID number – unless ID legislation over-rides	Better?

Technical and legal capacity for expanded uses The Australia Card system's technical capacity to expand the uses it could support depended on the expandable capacity of the central register, not that of the Card itself. With a smart card, this depends on the storage capacity of the card as much as the expandability of the back-end capacity. The additional capacity of the chip (beyond the original list of required functions) is not clear.

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. The government has apparently not yet decided even whether it will introduce legislation to legitimate the new ID system[9], let alone whether such legislation would restrict requirements to produce the card, or new uses of the ID number[10],

The card-holder's rights

The card-holder's rights to access and correct their own information seem much the same for both the 2006 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, because the current proposals do not include even the modest restrictions on expanded content and functions of the card or its use contained in the Australia Card Bill (as discussed above), the overall protection of card-holder's rights is far more uncertain.

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/change [some] own details online (Case Study – Family)	Better?
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

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 2006 proposal. In fact, the resemblances are

[9] See Mr Bashford (DHA): "It is not clear yet whether there needs to be legislation." Senate F&PA Legislation Committee Estimates, 25/5/06, F&PA (proof)

[10] See exchange between Mr Bashford and Mr Leeper (DHS) and Senator Stott-Despoja, Senate F&PA Legislation Committee Estimates, 25/5/06, F&PA (proof), which indicates the government has no proposals as yet

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', the saying goes[11]. The Australia Card ended up a dead duck. Whether this one takes flight remains to be seen.

References

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

Chadwick, Paul 'The value of privacy' Law Week 2006 address, State Library of Victoria, 23 May 2006; available at <http://www.privacy.vic.gov.au/>

Clarke, Roger (1988) '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, Peter (1990) Bureaucratic Politics and Technology: Computers & the Australia Card (Nathan: Centre for Australian Public Sector Management, Griffith University 1990)

Greenleaf, Graham (1987) '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, Graham (1988) '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>

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

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

[11] Well, almost …. James Whitcomb Riley (1842-1916) is attributed <http://en.wikipedia.org/wiki/James_Whitcomb_Riley> as saying ""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."