

'Access All Areas': Function Creep
Guaranteed in Australia's ID Card Bill (No. 1)

Graham Greenleaf*

*University of New South Wales

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

<http://law.bepress.com/unswwps-flrps/art11>

Copyright ©2007 by the author.

'Access All Areas': Function Creep Guaranteed in Australia's ID Card Bill (No. 1)

Graham Greenleaf

Abstract

Australia's Federal Government introduced into Parliament the Human Services (Enhanced Service Delivery) Bill 2007 on 7 February 2007 to establish its 'health and welfare access card' ID system. The Bill is only half of the blueprint for the ID system: the other half is yet to come in a Bill or Bills not yet seen. In this article I argue that the current Bill, and the government's 'access card' proposals as we currently understand them, should be rejected by the Parliament. The principal reason for this is that, despite the government's often-stated intention that they will not create a national identification system, there is an overwhelming likelihood that they will they will, and they should therefore be rejected. The existence (or likely development) of a national ID system does not depend simply upon whether a person is required to carry an ID card at all times, but depends upon an objective assessment of a number of factors, including whether one ID card and/or its associated ID number is likely to become predominant in use for identification purposes, effectively supplanting most other identification documents for daily purposes.

This article argues that the Bill will facilitate continuous 'function creep' in the use of the 'access card' and its associated ID number and other information. The ways it does so include (i) discretions in the Secretary and the Minister to make decisions expanding the system which are not disallowable by Parliament; (ii) objectives encouraging uncontrolled use; (iii) inclusion on the chip of capacity beyond what is needed for legitimate government purposes, with very little proposed control over how it can be used; (iv) lack of precision in when use of the card may be required; (v) inadequate offences controlling requirements to produce the card; (vi) inadequate offences controlling copying of information on the

card and in the chip; (vii) inadequate control over changes in business and government identification practices that make it inevitable that the card and number will be routinely offered for identification ('pseudo-voluntary production'); (viii) absence of controls over who will be able to access information in the Register; and (ix) no provision for payment of damages to cardholders for breaches of the Act. These inadequacies make it close to inevitable that the 'access card' system (including the Register) will develop into a national identification system, contrary to the government's promise to the Australian people, and contrary to their interests.



‘Access all areas’: Function creep guaranteed in Australia’s ID Card Bill (No. 1)

Graham Greenleaf*

Draft - *Submitted for publication to the Computer Law and Security Report, UK*

27 February 2007

Revised copies will be at http://www.cyberlawcentre.org/privacy/id_card/

Contents

ID cards in Australia – an ongoing debate	2
The open objectives of Bill No 1	2
The Register	3
Excessive content – photos, ‘interim’ IDs and the POI ‘honey pot’	3
Opportunities for function creep.....	4
The Card – on the surface	4
Excessive content will expand use	5
Expansion and control of card surface content.....	5
The Card – in the chip	6
The ‘Commonwealth area’ – unprotected content, more function creep?	6
The misleading idea of ‘your area’ of the chip.....	7
The encouragements to produce and record.....	8
Offences and illusions	9
Requirements to produce	9
Copying and using information from a card.....	10
The ‘ownership’ farce.....	11
The result: Pseudo-voluntary production and routine copying	11
Is the worst yet to come? (Bill No 2)	11
The Twilight Zone: The cardholder’s, doctors’ and other areas of the chip	13
Conclusions	13
This Bill should not pass	13
Still a national ID card?.....	14
References	14
Appendix: Amendments which would make the Bill less dangerous.....	16

* Professor of Law and Co-Director, Cyberspace Law and Policy Centre,, UNSW Faculty of Law; email g.greenleaf@unsw.edu.au; Thanks to David Vaile, Jan Whitaker and Abi Paramaguru for valuable comments; responsibility for the content remains mine.

ID cards in Australia – an ongoing debate

Australia's Federal Government introduced into Parliament the *Human Services (Enhanced Service Delivery) Bill 2007* on 7 February 2007 to establish its 'access card' ID system. The Bill is undergoing five weeks investigation and report by a Senate Committee, before Senate debate. The Bill is only half of the blueprint for the ID system: the other half is yet to come in a Bill or Bills not yet seen. I have argued previously (Greenleaf 2006b) that the 'access card' proposal carried with it the same dangers as the 'Australia Card' proposal rejected by Australians twenty years ago, but is more dangerous because of its greater technical sophistication. This paper continues that analysis in light of the Bill now released, with a particular focus on the dangerous opportunities for 'function creep' that the Bill provides.

The 'access card' scheme remains extremely contentious and the Bill's passage is not a certainty at the time of writing. A draft Bill was released just before Christmas 2006, and the Department of Human Services (DHS) received over 100 submissions, including a very critical one from its own Consumer and Privacy Taskforce (Taskforce 2007). The government previously rejected the most important earlier recommendations by the Taskforce (Greenleaf, 2006b). Four government MPs have publicly raised doubts about the proposal, one former Minister even stating 'it fails the Nazi test'¹. The Labor Opposition is still hedging its bets, posing criticisms but not yet declaring outright opposition. Press comment is often critical and detailed, and usually treats the government's continued claim that 'this is not an ID card' with scepticism. The report of the Senate Committee will be the next important development.

In this article I make numerous criticisms of the Bill. I have included in an Appendix a list of amendments to the Bill which would make it less dangerous, though still misconceived.

The open objectives of Bill No 1

The stated objects of the Act (cl 6) are to reduce complexity in accessing federal government benefits, reduce fraud concerning them, to improve access to emergency relief, but also 'to permit access card owners to use their access cards for such other lawful purposes as they choose'. Somewhat inconsistently with this last object, the government's insistence that this is not an ID card is stated: 'It is also an object of this Act that access cards are not to be used as, and do not become, national identity cards'. Since 'national identity cards' are not defined, this is largely meaningless. It is not a promise; at best it is a very vague guide to statutory interpretation.

A principal theme of this paper is that the Australian government is building an identification system through legislation which allows numerous opportunities for expansion of functions far beyond those stated to be its purpose ('function creep'). Whether we choose to call this a 'national identity card' will be a matter of definition, but it will not be what Australians have been led to believe this system is about, and it will be dangerous to their interests.

The card will be named at inception the 'Health and Social Social Services Access Card' (cl 27(1)). But if its purposes are so fixed and limited, why can the Minister change the name of the card at any time (cl 27(1)), and without Parliamentary scrutiny (cl 27(5))? A change of

¹ Senator Bronwyn Bishop, interview on ABC Radio 'Life Matters' programme

name will be able to reflect any expanded functions. For example, it could in future be re-named as the 'Australia Card'.

The Register

To obtain a card, anyone who is eligible for a Commonwealth benefit (which is pretty much everyone over 18) must apply to the Secretary of DHS for inclusion on the 'Register' (cl 13). They must provide particulars and supporting documents as decided by the Secretary (cl 13), in line with any 'identity guidelines' issued by the Minister (cl 66), so that the Secretary 'is satisfied of your identity' (cl 14). The Privacy Commissioner gets to 'comment' on this massive exercise in personal data aggregation (cl 13), but that is all.

The Register will contain about each cardholder their names ('legal', 'preferred' and aliases), title, date of birth, date of death, Australian citizenship or resident status, indigenous status, sex, contact details (residential and postal address(es), and on request phone number or email address), types of benefit card(s), registration status (current since when, suspended or cancelled; 'full' or 'interim' proof of identity), everything that appears on the face of the card (see below), a 'numerical template' of the photo that appears on the card, emergency payment number, and a flag identifying which participating agencies a person has a relationship with (cl 17). The register will also included copies of any of the documents that a person produced to prove their identity ('POI'), that the Secretary so chooses, and information about such documents (cl 17(1), item 12).

Excessive content – photos, 'interim' IDs and the POI 'honey pot'

The main problem with the Register is that which constitutes an accumulation of personal information which is unprecedented in Australia. Compared with this unprecedented nature of the register, and the dangers it presents, further function creep is a secondary matter.

First the Taskforce recommended that only photo templates should be included in the Register, not the actual photos (Taskforce 2006; see Greenleaf 2006b)). This has been rejected (cl 17, item 9(f)), so the Register will include the first national photo database. Second, it adds a national database of people's signatures (cl 17, item 9(g)). .

Finally is the astonishing power of the Secretary to include copies of any proof of identity documents in the Register remains in the Bill (cl 17(1), item 12), and stays beyond Parliamentary scrutiny (cl 17(2)). The Secretary therefore has the unreviewable power to decide whether to create an unprecedented POI database on every adult Australian, and to decide which classes of documents should be included in it. The Taskforce (2007a) castigated this as a broken undertaking, saying that it:

'does not believe that the *Draft Bill* reflects adequately the statements made by the Government in response to its recommendations (speech by Hon Joe Hockey MP, National Press Club, 8 November 2006) about the destruction of such records, either immediately they have been verified or at some subsequent time when their destruction will be part of a more ordered process.'

The Register's potential as a 'honeypot' for ID fraud and privacy invasion remains, and has been criticized on many occasions (eg Greenleaf, 2006, 2006a; APF 2007). The problem with item 12 of cl 17 is not that the Secretary has a discretion to decide what POI will be included in the Register for each individual, but that there should be any power in the Secretary to include POI copies in the Register at all. Item 12 should be deleted from cl 17 entirely.

The collection together of photograph, signature and an undefined range of POI create a system which is an exceptionally high security risk for identity fraud from unauthorized access, and also creates opportunities for future abuse by legislated changes to the system.

Finally, the register will include a unique identification number for each person (cl 17, item 9(a)), although the Bill does not define the number.

The Taskforce (2007a) criticised the draft Bill's inclusion of 'the place of your birth' in the Register, but this has now been removed (and rightly so, given its potential for prejudicial use).

Opportunities for function creep

One of the Taskforce's major criticisms (Taskforce, 2007) was the lack of Parliamentary or judicial oversight of the Register and its creation. Opportunities for discretionary decisions concerning the Register are provided in three ways, two of which give rise to dangers of function creep.

First, the Register itself is not a 'legislative instrument' (cl 16) and nor are the Secretary's determinations of specific aspects of its contents (cl 17(2)). They cannot therefore be disallowed by Parliament. Some of these determinations concern circumstances particular to individuals (cl17, items 2,3,7 and 8), and are therefore unsuitable for Parliamentary review. What these determinations require is an appeals mechanism, which is not included in this Bill. The Bill still allows for card suspension and cancellation (cl 17, item 8(b)) even though there is no appeals mechanism.

Second, the Secretary can determine 'other technical or administrative information' that 'is reasonably necessary for the administration of the Register or [the] access card', provided it 'does not expressly identify [the cardholder] by name or other personal identifier' (cl 17, item 17(a)). Any such determinations will escape Parliamentary scrutiny (cl 34(2)). Does the inclusion of 'expressly' mean that information indirectly identifying the cardholder can be included? 'The serial number of the chip' is given as an example of what can be included here (EM 2007), but queries have been raised as to whether this may allow individual identification². At the very least, this item should require the Secretary to determine the precise classes of 'other technical or administrative information' which are to be added, and for such determination to be disallowable.

Third, the Minister can determine to add 'other information' 'that is for the purposes of this Act', but must do so by legislative instrument (cl 17, item 17(b)). Parliamentary scrutiny is therefore possible, but only in the weaker sense of disallowance rather than requiring positive approval. The Minister's 'identity guidelines', in accordance with which the Secretary must act, are also legislative instruments (cl 66), so this gives some control at a level above the Secretary. However, given the width of the Bill's objects, this is too general a power to expand the Register. It should require new legislation.

The Card – on the surface

The information on the surface of the card is to be the cardholder's name ('legal' or 'preferred', provided it is not 'inappropriate'), card number (unique, but not defined in this

² Irene Graham, Electronic Frontiers Australia, email discussion list posting, 26 February 2007.

Bill), card expiry date, photograph, digitised signature, date of birth (if requested), and various items of benefit-related information which are optional ('Blind', 'POW', 'war widow' etc) (cl 30). All of this is also in the Register (cl 17, items 9,10 and 11).

Excessive content will expand use

As with the Register, the problem that the card will contain excessive personal data from the outset is more important than the possibility of the contents expanding. The Taskforce recommended no signature should be visible on the card (Taskforce 2006, recommendation 15) but the Government rejected this because it will 'make it easier to cross check signatures' on paper forms. The Taskforce also suggested that there is no need for the ID number to be visible on the card (recommendation 18), but the Government rejected this, to 'make it quicker and easier for people to use the card for telephone and online services'.

The Taskforce (2007a) criticised the voluntary inclusion of date of birth on the card face, as a new element not part of the original proposal and one which 'devalues the security protection of the card and materially enhances the opportunities for fraud and identity theft'. The government has ignored this advice and the consequence of the increased likelihood of fraud, in a system that has a professed object of reducing fraud. We could add to the Taskforce's objections 'and increases the probability of the card turning into a national ID card'.

The unnecessary aggregation of types of personal information on the card surface (photo, signature, ID number and date of birth), coupled with the presumed high level of authentication of these details, that does most to ensure that this will evolve into a national ID card.

Expansion and control of card surface content

The only content on the card surface can be that which is specified in cl 30 (cl 32). The potential for function creep arising from changes to the surface of the card is therefore limited because of the need for legislative change. However, the 'form' of the card can be determined by the Minister (cl 27(4)), without Parliamentary scrutiny (cl 27(5)). This could include the colour or shape of the card, and perhaps any decorations appearing on it, but the specificity of cl 30 implies that no other text could be included, at least not if it differed between individuals.

Which card-face data is machine readable (if any), by what means and by whom, does seem to be within the notion of the 'form' of the card, and is not otherwise specified by the Bill. This is a significant omission, and should be defined in the Bill. However, cl 57 (discussed later) does provide some protection against copying of card-face data.

The apparently closed provisions of cl 30 have already been undermined by the Taskforce (Taskforce 2007b) which now proposes that the card could contain on its surface 'some symbol (such as the caduceus) to indicate that emergency medical data is stored on the chip'. Since this won't be dealt with in Bill No1, it is already clear that Bill No 2 is likely to be expanding the scope of aspects of the scheme apparently defined and limited in Bill No 1. A consequential issue which the Taskforce does not discuss is whether, if a person chooses to have emergency medical data added to their card after the card is issued, a new card will have to be issued to them. If not, their card would be misleading (and potentially life-threatening) in that its surface would not indicate that it contains emergency medical data. This illustrates that apparently definitive aspects of the legislation are in fact only provisional.

We are likely to see more of this retro-fitting. Perhaps if a person chooses to use their card for financial sector applications, many of which are reportedly being planned, their card surface could have a '\$' symbol, which would be time-saving for Banks and fraudsters alike.

The Taskforce's criticisms (Taskforce, 2007) of the dangers of including titles (particularly the ambiguous 'Dr') on the face of the card have been heard, though titles are still included in the Register.

The Card – in the chip

Unfortunately for those who wish to understand what this ID system really means, this Bill only defines half of what can be on the chip (cl 33): that in the 'Commonwealth's area' but not in the card-holder's area ('your area' as the Bill puts it). As we will see, this bipartite division is quite misleading.

The 'Commonwealth area' – unprotected content, more function creep?

The 'Commonwealth's area' will include everything that is on the surface of the card, plus a lot more information including a person's 'legal name' (protected by their PIN) if the card shows their 'preferred name', sex, residential address, card expiry date, any PIN or password ('protected by encryption or other technological protection measure) used to protect information on the card-holder's area, information about benefit cards held (as determined by the Secretary), Medicare number, Reciprocal Health Care Card number, emergency payment number, whether the person's POI is 'full' or 'interim', and information about veteran's pensions (cl 34).

The main problem with the chip is that it contains a great deal of personal information, but we do not know who will have access to it. This Bill does not answer any of the questions about access to information in the Commonwealth area of the chip. Which data will be able to be read by anyone with a card reader? Which will be protected by encryption so that only those who have the Commonwealth's key (ie an 'authorised' card reader) can access it? The Bill requires only that a cardholder's legal name, and PIN number will be protected by some means, but cl 34 does not require any technical protection for the rest of the data in the Commonwealth area. Since cl 57 does not provide any legal protection at all against copying or use of information in the chip (see later), it seems that all of the other information in the Commonwealth area is not required to have any protection at all, technical or legal. Nor is there any indication that this is planned to be included in the second Bill (EM 2007).

A potentially very dangerous item on the chip is the designation on the chip of whether a person's POI is 'full' or 'interim' (cl 34, item 14), which is determined by the Secretary's discretionary power over the corresponding Register entry (cl 17, item 8). This could be seen as dividing Australians into those who are 'first class' (fully authenticated) and those who have been declared by the government to be 'second class' (suspect identity). Who is to have access to whether a person's identity is declared to be suspect, and what are they to be able to do with the information? No explanation is given (EM 2007). Will there be fair and adequate appeal rights? The Bill does not cover any of this. It may be necessary for some form of this information to be kept on the Register, but it is far more dangerous to put it into the hands of everyone who deals with a person's card and has access to data on the chip.

There is some potential for function creep in the government's part of the chip, because the Secretary can add new 'technical or administrative information' to the chip (cl 34, item 17),

without Parliamentary oversight. This has the same deficiencies as the similar clause allowing expansion of the Register (cl 17, item 17), as the Taskforce (2007) pointed out.

The misleading idea of 'your area' of the chip

The Bill asserts that 'the information in the chip in your access card consists of two parts': that in 'your area' and that in the 'Commonwealth's area' (cl 33). It is further explained that (EM 2007):

'It is proposed that card owner will be able to include in their area of the chip area any information that they choose to include (subject to the physical capacity of the chip and any legal restraints). It is expected that card owners will be able to customise their card to include additional information such as organ donor status or emergency contact details. To the extent necessary these matters will be dealt with in subsequent legislation.'

In these and other ways the government has created the impression that 'your area' will be under the cardholder's control. The Taskforce's Discussion Paper on emergency and medical information (Taskforce 2007a) shows that cl 33 is oversimplified and misleading. The Taskforce proposes 'a two-tiered system of emergency and health information'. The 'first tier' is to include 'only that data which is absolutely necessary [for] emergency health treatment in a crisis situation', which is to be 'accessible to anyone with an approved reader' and therefore 'effectively, [put] into the public domain'³. The 'second tier' can include 'other medical and health data', but will be PIN protected against access without consent. The Taskforce then recommends 'That no voluntary medical information be entered into any part of the access card without verification of the accuracy of that information by an approved medical or other practitioner.' It then underlines what it means, in flat contradiction of the Explanatory Memorandum:

'This has a clear implication that the entry of such information cannot be done by the individuals themselves since this would allow the bypassing of the verification process. It means, at least for Tier 1 information, data entry can be done only at an approved location and only from an approved and authenticated form'.

While the Taskforce's recommendations are not clear in relation to its 'Tier 2', it is the Government's own advisory body, and what it says is the best current guide to what the legislation will provide concerning 'your area' of the chip. The implication of its recommendations are that there are at least three very separate parts of the chip, one of them being the part to which only 'an approved medical or other practitioner' can write data. Furthermore the 'Tier 1' part of the chip (which may be only a sub-art of the doctor-writeable part), will have quite different access conditions than 'Tier 2' which is PIN-protected. At the least there will be three distinct parts to the chip: the Commonwealth's part, 'your part', and 'your Doctor's part'. A more detailed critique of the Taskforce's recommendations is not needed here. From what has been said, it is obvious that a subsequent Bill will impliedly change s33, whether this is admitted or not, and that the Bill and its Explanatory Memorandum are likely to be shown a future Bill to have been misleading. This is a misleading and inappropriate way to pass legislation.

³ Despite this 'public domain' comment, the Taskforce makes the seemingly inconsistent comment that the highest priority must be given to 'ensuring that there are effective sanctions available and applied in relation to people and organisations who breach privacy requirements inherent in the management of sensitive data'. This is one example of the complex legislative balancing act that the unseen second Bill will apparently have to include.

Why does the Bill fail to define the cardholder area of the chip? The government could try to justify this by the fact that it was waiting for the Taskforce's recommendations, but does not (EM 2007). It is plausible that its omission is a strategy of withholding controversial features from the first Bill, or alternatively an admission that the government hasn't yet worked out how it will manage the enormous security and privacy challenges, and costs, of the cardholder's portion of the chip. Whatever the reason, the Bill's implications cannot be understood until this is dealt with. This is discussed further below.

The encouragements to produce and record

The Bill goes out of its way to facilitate as wide a range of uses as possible of the card, while maintaining the pretence that such uses will be voluntary. To start with, 'access card' is defined to include the chip in the card (cl 5), so the seemingly innocuous references to uses of the 'access card' also allow uses (such as copying) of the information contained in the chip. This is a very dangerous definition because people may consent to uses of their 'access card' thinking that this means what is visible on it, but find they have given far broader consent.

Card-holders are expressly entitled to use the card 'for any lawful purpose' (cl 40), so no use that any other organisation makes of the card can be argued to be *per se* improper or unlawful, unless this Bill or some other legislation makes it so.

'Participating agencies' (six are defined) are only entitled to use the card for the purposes of this Act, or for any other purposes if they have the card-holder's consent (s41). While this imposes more restrictions on them than on other parties, there is nothing to stop Centrelink or other participating agencies adopting a policy of requesting all their clients to consent to other uses of the card (and therefore the information on the chip). Provided they allow their clients some other way of satisfying their request (so as not to breach this clause or cls 45-46), they can take the initiative to expand the functions of the access card. That this can occur even within these agencies that will have access to the Register is doubly dangerous. If this form of function creep is to be avoided, then cl 41 should be restricted to situations where other uses of the card are at the express request of the cardholder and with their written consent. 'Consent' is not enough protection.

Any other agency or organisation is free to use the information for purposes that do not require the card-holder's consent, provided it can obtain the card (see below concerning cls 45-46) and it can copy the information it wants from the chip (see discussion above). It may be prohibited from copying and using the information *on the card surface* without consent (see below concerning cl 57 and its limitations). If access can be obtained to information on the chip (and therefore outside s57), then despite the *Privacy Act 1988* there will be a wide range of 'legitimate' uses which do not require consent (though the law of breach of confidence may sometimes impose limitations). A non-exhaustive list of examples includes any secondary purposes allowed by privacy principles (IPP 10 and 11 or NPP 2), any of the other exceptions to those privacy principles (for example, any further disclosures 'authorised by law'), and of course any uses of the information by organisations in the 'privacy-free zones' of 'small businesses', political parties, some uses by employers, and so on. If a State agency obtains access, no privacy legislation will apply in most States.

It is therefore simply not the case generally that the information on or in a person's card can only be used for access to benefits or for uses that the card-holder voluntarily chooses. Once a cardholder allows an agency or organisation to use their card, their control over the information on or in it may vanish. It may be the case that 'if you use it, you lose it'.

Offences and illusions

The Bill includes a number of offences which, as will be shown, are illusory in many situations. They will not provide sufficient protection against use of the card, or the information in it, for purposes other than those for which it is required, or those that are expressly desired by the cardholder. Since prosecution for offences is not under the control of the person whose card or information is misused, offences can at best be only part of the remedy needed.

The Bill omits any provision for civil compensation claims for misuse of the card, or the information in it, and the government has not stated any intention to include compensation in the second Bill (EM 2007). The only remedy available would be a complaint to the Privacy Commissioner, but since the Commissioner has only ever made one contested award of compensation in nearly 20 years of the *Privacy Act's* operation, and there is no appeal against the Commissioner's decisions, this is not a sufficient remedy. It is also not certain that a breach of this Bill's provisions would constitute a breach of the *Privacy Act*, though it is possible. People whose cards (or information in them) are misused should be able to go directly to a Court and obtain compensation.

Requirements to produce

When is an agency or organisation (other than a participating agency) prohibited from obtaining a person's card? Another party (for example a doctor) can require a card-holder to produce a card to identify themselves to establish that they hold a benefit card or medicare number. Otherwise, it is an offence to require a person to produce their card for identification purposes (cl 45(1)), and an attempt is made to prevent implied requirements (cl 45(2)). It is similarly an offence to expressly or impliedly require a person to produce a card in connection with the provision of a widely-defined list of benefits (cl 46).

There are two significant problems with these apparently broad offences. First, why do they simply not prohibit a person being required to produce a card for 'any other purpose' than those expressly allowed? The enumerated list, while extensive, is an invitation for organisations to find loopholes, and does not have the psychological clarity to cardholders and potential users of a prohibition for requirements to produce for 'any other purpose'. If that is what the Bill means, it should say so. If it is desirable to have a list of examples such as in cl 46 in order to underline the point (as the EM 2007 suggests), these can best be included as a note in the Bill.

Second, since the Crown (in the Commonwealth, States, ACT and NT) is bound by the Act but immune from prosecution for an offence under the Act (cl 9(2)), what effect do the offences have in restraining wrongful demands by Commonwealth or State/Territory agencies? It appears that any individual officers who breached these sections would also be immune from criminal proceeding⁴. Offences by individual Commonwealth officers are defined (cl 61 and 62), but they do not include wrongfully demanding a card. What remedy does an ordinary person have if a government agency in a State requires them to produce their card? It is likely that a Court would refuse to exercise its discretion to even make a declaration that the Crown or its employees should comply, given that they are immune from

⁴ See for example *Laing v Carroll* [2005] FCAFC 202, where in similar circumstances it was held that 'State employees, through whom a State acts, cannot be prosecuted'

prosecution⁵. It seems the cardholder could only seek judicial review of administrative action, which is a very weak remedy indeed. There is no provision for cardholders to even seek compensation. The conclusion must be that cardholders are left defenceless against wrongful demands for production by the Crown, including by State and Territory government agencies.

The broader criticism of these offences is that they can easily be side-stepped in any event, simply be an organisation or agency refusing to accept successively proffered items of identification until a person 'voluntarily' produced their 'access card' in desperation. There does not have to be any uniform policy of refusing other IDs, a severe contraction of what was regarded as acceptable IDs would rapidly have the effect that everyone would start proffering their 'access cards' in order to avoid the annoyance of refusal. It is doubtful that this could be proven to breach cl 45 or 46 on a criminal standard of proof, unless the organisation concerned was stupid. What prosecutor would want to take on this burden of proof? In the Australia Card debates this was called 'pseudo-voluntary production' (Greenleaf, 1987), and it is the same today.

Copying and using information from a card

If a cardholder produces their card to an agency or organisation (other than a 'participating agency') what is to stop details on or in the card being copied, used or disclosed? This depends on whether we consider information on the surface of the card or in the chip.

It is an offence to copy or record a person's number, photograph or signature '*on the surface* of an access card' (cl 57(1)), or to 'divulge or communicate it', or if a person 'uses it in a manner connecting it with the identity of the owner of the access card', unless written consent is obtained (cl 57(2)). The restriction on use does not prevent all uses of a card which has been presented. The cardholder's name and the fact that they hold a card, their date of birth, any recorded status (POW etc) can all be recorded. Otherwise, the meaning is not clear.

Otherwise, to copy (etc) a person's number, photograph or signature *on the card surface* require written consent (cl 57(2)). This is more protective than allowing verbal or implied consent. However, all any private sector organisation has to do is to include in a standard form a provision that, if you (voluntarily) produce your card to them, then you consent to their copying it and making specified uses of the information. Government agencies, whether Commonwealth or State, do not even have to go to that trouble, as they are immune from prosecution (s9(2)). The protection is to a large extent illusory, at best a slight inconvenience for the private sector.

Alarmingly, there is no equivalent offence to s57 in relation to the copying of any information *in the chip*. The far more extensive information in the chip is left unprotected by law from copying, use and disclosure. This is a major hole in the Bill's protection, which is not explained (EM 2007). As discussed earlier, the protections in other aspects of the law against subsequent (mis)uses are thin and unreliable. Given the hole in the offences concerning data on the chip, the technical questions of how each item of data on the chip will be protected (by encryption or otherwise), and who will have 'authorised' readers, assumes even greater importance. It is left unanswered by this Bill (see below).

⁵ in *Laing v Carroll* [2005] FCAFC 202 the Court refused to exercise its discretion to make a declaration that a State employee should comply with a notice, when the Crown was immune from prosecution for failure to comply.

As with all other offences in the Act, the Crown (Commonwealth, State and Territory agencies and their employees) are immune from prosecution under cl 57. Most State and Territory governments are also not inhibited by information privacy binding them. It is hard to see how they can be restrained once a card is presented to them.

Assuming agencies do comply with cl 57 despite not being liable to prosecution, the ability of the Secretary to authorise who can copy, use or disclose data on the card has been considerably reduced from the draft Bill, at the behest of the Taskforce. It is now subject to disallowable regulations and a continuing requirement that information be used for the purposes of the Act (s72).

The 'ownership' farce

The Bill's ostensible granting of 'ownership' in the card is a joke and a deception. 'You own your access card' trumpets cl 37. But cl 38 quickly adds

'However, subsection 37(1) does not give you ownership of any intellectual property or information that, at any time, is on the surface of, or in the chip in, your access card that you would not otherwise have.'

In other words, a cardholder owns the plastic card, the chattel, but nothing else. Even this is effectively rescinded by cl 50-53 which criminalise any attempts by the cardholder to amend, destroy or sell 'their' card. Rights to modify, destroy and alienate are among the normal incidents of ownership of chattels, and if they are all removed 'ownership' means next to nothing. At least if you were somehow given some exotic property right in the information content of the chip you could claim that any copying was a breach of your 'ownership'. But cl 38 denies this, and the poor cardholder probably does not even have any copyright in information in the 'gobbets of fact' in the cardholder part of the chip (unless they store haiku there), let alone in the new 'doctor' part where they cannot even enter the data. The s37 grant of ownership may give a cardholder some theoretical remedy for conversion of goods against a Commonwealth officer confiscating their card without legal authority, but it is hard to see what else it adds to the law, and the Bill does not explain (EM 2007). Legislation should not include deceptive stunts like this.

The result: Pseudo-voluntary production and routine copying

This Bill claims to forbid a person being required to produce their card, or allow their information to be copied, for anything other than a very narrow range of intended purposes, but to allow voluntary uses for other purposes. In doing so it is very similar to the Australia Card proposal. However, we have now seen that this 'voluntariness' can be made illusory. The protection against private sector organisations requiring a production of a card is based on a list that may have loopholes, and in any case can be side-stepped by a practice of accepting few other ID documents. There is no protection against copying data on the chip, and the protection against copying card-face data is easily avoided by a bundled consent. Governments need not even bother side-stepping, as they are immune from the offences.

If the Bill is not significantly strengthened, the result will very probably be that the card, and the information in it, will be routinely available for any uses that the public sector, in all jurisdictions, or the private sector, wishes to make of it. It will become a national ID card.

Is the worst yet to come? (Bill No 2)

This Bill is dangerous enough, but does not cover many crucial aspects of the proposed system. They could have very adverse effects on the interests of Australians, but are being

saved for a second or third Bill, if they are to be covered at all. The Explanatory Memorandum to the Bill includes only some very cursory indications of what a subsequent Bill might include (EM 2007, 'Matters not dealt with in the Bill), and the Department has provided few additional details. Some of the more important outstanding issues are now noted.

Will there be adequate rights to challenge the refusal or cancellation of a card? – Life in Australia will be likely to be very difficult for anyone without an access card. Will there be fair review procedures where individuals wish to challenge the Secretary's decision that they cannot have an access card, because their proffered POI does not meet the required standard of proof that they exist? What are the implications of POI being declared to be in the limbo of 'interim' and is that reviewable? How and how quickly will the suspension or cancellation of a card be reviewable? What happens to the 'voluntary' aspects of the card in that eventuality? So far, the Bill lacks any definition of administrative or judicial review, there is only a promise that it will exist (EM 2007, p51). These matters go to the heart of the access card system and the fairness with which it will operate.

What penalties will apply to card replacement? - People lose wallets, handbags and cards by the thousands every day. ID cards are also very valuable to potential fraudsters. We can assume that there will be some penalties for lost or stolen cards, as a deterrent against attempts at 'identity fraud'. This administrative tension is potentially harmful to individuals who genuinely lose their cards. Lack of definition leaves people's interests exposed, particularly the interests of those least able to look after their own affairs.

How harshly will the card requirement be applied from 2010? – There is no possibility that every Australian with disadvantages caused by ill-health, mental disability, language difficulties, remote location, or living on the street will obtain an ID card by 2010 when it is to be necessary to present a card to get benefits. How will the Bill define the latitude that agencies will have in denying people the means to live because they own no card and have no identity?

What privacy protections will be provided? – There is a vague statement that 'privacy issues' will be 'fully considered' in Bill No 2, coupled with an worthless assurance that 'the whole suite of existing legislative privacy protections will apply the card and Register' (EM 2007). Such statements purport to recognise that this scheme cannot possibly be in the interests of Australians without sufficient privacy protections being included, while at the same time refusing to define what they will be. The statement also ignores that fact that everything that the Bills allow will override any protections found in the *Privacy Act 1988*, because they will constitute 'authorised by law' exceptions. Lack of full and precise details on this point makes the legislation illegitimate.

Which agencies will have access to the Register? – There is nothing in the first Bill to protect the Register against accesses for any purpose. Access will continue to be 'governed' by the *Privacy Act 1988*. That protection is illusory because the 'authorised by law' exception to IPP 11 means that agencies with general demand powers will be able to exercise them over the Register's content. The legislation must define which agencies may have access to information in the Register and for what purpose, and allow no expansion except by further legislation. Otherwise, there is no effective protection against function creep in the uses of the Register.

Will individuals be able to access what the Register says about them? – The first Bill does not guarantee this. It's easy to assume it will happen, but unless the second Bill provides a mechanism, access will be ineffective. Reliance on the formalities of the FOI Act would be inappropriate and inadequate here.

Will individuals know who has access to their records? – The first Bill does not guarantee that individuals can find out which agencies access their records on the Register, and the government has refused to give a commitment (SMH 8/2/07).

How will the card number be determined? – Will it be random or will it imply information about the person? Will it change every time a card is issued, or will it stay with you for life (even if your card is stolen)? This is important, particularly in relation to the likely development of a national ID system, but the legislation guarantees nothing at this stage.

The Twilight Zone: The cardholder's, doctors' and other areas of the chip

The first Bill defines what will be on the 'Commonwealth's area of the chip', and declares there will also be 'your area of the chip' (cl 33), but does not say what will be there. We have already seen in relation to medical and emergency information that this is likely to be an extremely complex question, and that it means there is to some extent a 'doctor area' of the chip. This potential use of this chip capacity is one of the most contentious aspects of the ID scheme. Many organisations which the government wants to support the proposal are vying to have the second Bill facilitate the 'voluntary' inclusion of information to serve their interests. Many of the worst privacy dangers, and the forms of function creep which will lead to a far more comprehensive ID system, may come from these potential inclusions (see Greenleaf, 2006, 2006a, 2006b for examples).

At this stage even the chip size, which to some extent determines the possible additional uses of the card, is not disclosed, or specified by the Bill. The Taskforce (2007b) states in relation to the cardholder part of the chip:

The exact amount of space (chip capacity) which will be available has yet to be determined but will be approximately one-third of the entire chip. Thus, the space available will depend on whether the chip specified in the card is of 64 kb capacity or some larger amount. In a 64 kb chip the customer controlled area will be in the order of 20 kb.

This leads to the next question.

Who can read what information on the chip? – There is a lot more information on the chip than on the face of the card, and it can be read and copied by computerised means. Little of it is required by the first Bill to be encrypted or protected by PINs or passwords. Provided someone observes the very limited legal restrictions (discussed above) on obtaining and copying card information, then anyone with a card reader can theoretically obtain a lot of personal information. What information in the 'Commonwealth area' will be encrypted, and who will have readers that can read it? There are major question of both technical data security and legal guarantees of data security yet to be dealt with.

Conclusions

This Bill should not pass

The government's tactic appears to be to get the first Bill through, which is probably enough to make the scheme unstoppable. If the second Bill contains a lot of bad news for privacy protection, it will be too late for any Parliamentarians to have second thoughts about the

passage of the first installment, and the government may be able to live without the second Bill if it has to. This is a dangerous and unreasonable approach to the passage of legislation. The implications of many of the provisions of Bill No 1 cannot be understood except in the context of matters not included in that Bill. These include rights of appeal and judicial review, the consequences of replacing lost or stolen cards, who can access the Register, which card readers will be able to read which aspects of the chip, and the penalties for hacking information on a chip. How is it possible for anyone to support the passage of this Bill while the legislative details of these crucial matters remain unknown, and (even worse) the government has not even announced an intention in principle to deal with some of them.

The government's proposal that this Bill should be passed now can reasonably be described as a confidence trick. The Parliament should defer any decision on passing this Bill until legislation covering all aspects of the 'access card' proposal is before it.

Still a national ID card?

The quarterly examinations I have made of this scheme since it was announced (Greenleaf, 2006, 2006a) led me to conclude that there was little to distinguish the 'access card' scheme from the rejected Australia Card of the 1980s, except that it was far more dangerous than that primitive proposal. Nothing in this Bill changes my views. The duck quacks louder with every iteration. This Bill has the capacity for function creep built in to all aspects of the system. Too many are being put beyond Parliamentary control. The Bill lacks meaningful protections against such expansion. It will lead to a national ID system.

References

Australian Privacy Foundation 2007 *Submission to DHS - Draft Access Card Bill of December 2006* 12 January 2007

Greenleaf, G. 2006b 'Australia's Proposed ID Card: Still Quacking Like A Duck' *Computer Law & Security Report*, Vol. 23, 2007; UNSW Law Research Paper No. 2007-1, at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=951358>

Greenleaf, G. 2006a '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, G. 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>>

EM, 2007 *Human Services (Enhanced Service Delivery) Bill – Explanatory Memorandum*

Human Services (Enhanced Service Delivery) Bill 2007 at <http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=2450&TABLE=BILLS>

Taskforce 2007 [Access Card Consumer And Privacy Taskforce] *Submission To The Department Of Human Services Human Services (Enhanced Service Delivery) Bill 2007 Exposure Draft*, January 2007

Taskforce 2007a [Access Card Consumer And Privacy Taskforce] *Discussion Paper No 2: Voluntary Medical and Emergency Information*, 21 February 2007

Taskforce (2006) - 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 <<http://www.accesscard.gov.au/publications.html>>



Appendix: Amendments which would make the Bill less dangerous

The submissions in the paragraphs following propose specific amendments to the text of the Bill. Even if all of them were adopted this would not constitute good enough reason to support the Bill, because its objectives are flawed. The better course would be to abandon this Bill and start again, in order to develop legislation as suggested in the previous submission. These proposed amendments are merely to indicate what is necessary to make this Bill less dangerous, and in particular to reduce the likelihood of its development into a national identification system. Brief reasons for each suggested amendment are given in italics, referring back to the explanation in the preceding article.

- 1 In cl 5, amend the definition of 'access card' by replacement of the words 'and includes' with 'but does not include'.
If the chip and its contents are included in the meaning of 'access card', people will agree to things without realizing the scope of what they have agreed.
- 2 Delete cl 6(1)(e)
Permitting the use of access cards for purposes completely unrelated to Commonwealth benefits should not be an object of this Bill (even if it is a side-effect), and makes it impossible to prevent function creep if it is an object.
- 3 Add to cl 9 a new sub-clause (3): 'Despite s9(3), any Commonwealth officer or an officer of a State or Territory government commits an offence if that person does any of the acts that constitute an offence under this Act'.
Agencies must be prevented from abusing access cards. Even though the Crown cannot commit offences, individual officers can. There must be a deterrent to abuse.
- 4 Delete cl 17(1), item 12
- 5 Amend cl 17(2) so that it only applies to items 2,3, 7 and 8.
These decisions by the Secretary should be disallowable by Parliament, except in relation to items 2,3, 7 and 8.
- 6 In cl 27(1) delete the words 'or such other name as the Minister determines in writing'
A change of name would indicate function creep and should require new legislation.
- 7 Cl 24 should define which items on the card-face are machine-readable, and by which means. Alternatively (but not preferably) add to cl 27(4): 'The Minister shall include in any such determination specifications of the machine-readability of any item of information on the access card.'
The machine-readability of card information should be defined in the Bill, or at the least be part of a disallowable determination.
- 8 Delete cl 27(5)
Changes to the form of the card (including to its machine-readability) should be disallowable.



- 9 Delete cl 30, item 6
Date of birth should not be included on the card face, as it will facilitate fraud and the use of the card as a general ID card.
- 10 Delete cl 34(2)
Any changes by the Secretary to information in the Commonwealth's area of the chip should be disallowable.
- 11 Add replacement cl 34(2): 'The content of the Commonwealth area of the chip will be protected by the highest strength of encryption which is practicable.'
The content of the Commonwealth area should not be able to be read by anyone who is not authorised to do so and who does not have a card reader with the Commonwealth's decryption key. This will assist in discouraging function creep.
- 12 Amend cl 40 by addition of the words 'but you cannot be required to use it or produce it for any purpose other than the purposes for which its use is required by this Act'.
If this is the intention of the Bill, cl 40 should say so. This would underline the supposed intention of cl 45 and cl 46.
- 13 Amend cl 41 by re-numbering it as cl 41(1), and by replacement in (b) of the words 'with your consent' by the words 'at your express request and with your written consent'.
This will ensure that proof of consent is held by Commonwealth agencies, and will assist in preventing function creep in the use of the card. Otherwise, practices will develop where Commonwealth agencies expect people to allow their cards to be used for non-required purposes.
- 14 Add a new Part 3 Division 7 'Compensation for misuse of your access card'
The Bill does not make any provision for cardholder's to obtain compensation for misuse of their cards or the information contained in or on the card. The following proposed section would provide such a right to compensation, which could be pursued either by complaint to the Privacy Commissioner, or directly before a Court.
- 15 Add a new cl 42A as follows:
- '(1) You are entitled to obtain compensation from any person if that person:
- (a) uses your access card in breach of section 41(1); or
 - (b) requires you to produce your access card in breach of section 45; or
 - (c) does, in relation to your access card, acts that constitute any offence under this Act.
- (2) You may claim compensation for a breach of this section by the same procedures as you may claim compensation for an interference with your privacy under the *Privacy Act 1988*, or by civil proceedings in any court of competent jurisdiction.
- (3) In any proceedings under this section, it is only necessary for you to satisfy the civil standard of proof, including in relation to proving that a person has done the acts that constitute any offence.

(4) There is no limit on the amount of compensation that may be paid to you under this section.

(5) Where a person purports to act on behalf of the Crown, the Crown is liable to pay any compensation to which you are entitled under this section.'

16 Amend cl 45(1) by replacement of the clause with the following:

(1) A person commits an offence if the person requires you to produce your access card or someone else's access card for any purpose unless

(a) if the person is a *delegate or an *authorised person—the requirement is made for the purposes of this Act; and

(d) if the person is not a delegate or an authorised person—the requirement is made for the purposes of the administration of *benefits or payments related to medicare numbers to establish that:

(i) you hold, or someone else holds, a *benefit card; or

(ii) you have, or someone else has, a *medicare number.

Penalty: Imprisonment for 5 years or 500 penalty units, or both.

17 Delete cl 46

Amendment of cl 45 and deletion of cl 46 will make it very clear that no one can require production of an access card except for the purposes required by this Bill. If the above drafting omits any such purposes, they should be explicitly added after (d)(ii). The current drafting of cl 45 and cl 46 is obscure and invites exceptions to be found.

18 Delete cl 54(1)(b)

A person's ID card should not be liable to forfeiture because they have used it in relation to some offence that has nothing to do with the objects of this Bill. This would allow forfeiture of the ID card wherever a person merely used it to identify themselves during a course of conduct involving an offence, even though it bore no other relationship to the offence. This is using forfeiture of identity documents as an additional sanction for offences.

19 Amend cl 57(1)(a) by adding after the words 'on the surface' the words 'or any information in the chip'.

Information in the chip should at least have the same protection as information on the card face.

