Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Function creep - defined and still dangerous

Submission on the revised ID Card Bill

(Human Services (Enhanced Service Delivery) Bill 2007)

Graham Greenleaf *

25 August 2007

Contents

A defective Bill, version 2 – one step forward, two steps back 2
The inappropriately open objectives of the Bill 3
The 'ownership' farce 4
The Register 4
Opportunities for content expansion (function creep) 5
The uncertain position of POI data 5
Excessive content – photos, contact and location data, and 'interim' IDs 6
The so-called 'emergency' payments number 6
The Card – on the surface 7
Excessive content will expand use 7
Expansion and control of card surface content 7
No protection against copying of card face data 8
The Card – in the chip 8
Content of the chip 8
Function creep in the chip's content 9
Has 'your area' of the chip disappeared? 9
Inadequate legislative requirements to protect chip content 10
Access to the card - Encouragements to produce and record 11
Inadequate offences for requirements to produce 11
Uses of a card, once produced 13
Special protection for ID numbers 14
Access to the Register – Enshrining the 'honeypot' for investigators 14
Unjustifiable lack of civil remedies 15
Does this Bill cover everything it should? 15
Conclusions - Still a national ID card, and should be rejected 16
References 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, Abi Paramaguru and Nigel Waters for valuable comments; responsibility for the content remains mine. Some content of this submission, particularly that relating to identification numbers and NPP 7, derives from research done for the Australian Research Council Discovery project, 'Interpreting Privacy Principles', see <http://www.cyberlawcentre.org/ipp/>.

A defective Bill, version 2 – one step forward, two steps back

This submission does not examine every aspect of the Exposure Draft of the *Human Services (Enhanced Service Delivery) Bill 2007*. It concentrates on those aspects of the Bill which (directly or indirectly) determine the scope and purposes of the identity system which it will create, and in particular what opportunities they provide for expansion of those functions and purposes beyond those the government claims the Bill is about. In other words, this is a submission principally about the opportunities for function creep. Although in this submission I put forward some detailed recommendations for how the Bill could be improved, that is not an endorsement of any Bill containing such improvements, first because I have not attempted to be comprehensive, and second because the Bill is still fundamentally flawed in its objectives and methods, as many other submissions argue, and should be abandoned in favour of a more limited and less dangerous approach.

In summary, my detailed conclusions are:

- The objective in cl 7(1)(e) 'to permit access card owners to use their access cards for such other lawful purposes they choose' should be deleted.
- The Minister should not be allowed to change the name of the card (cl 67(1)) , this should require legislation.
- The Bill's ostensible granting of 'ownership' in the card is deceptive, and should be deleted from the Bill.
- Clause 35 item 18, allowing expansion of the Register's content by Administration Rules, should be deleted. Similarly, cl 74 item 17 allowing expansion of chip content should be deleted. Both such forms of function creep should require new legislation, not merely disallowable delegated legislation.
- The content of the Register is already excessive, and should be reduced to the minimum necessary for the legitimate objectives of the Bill.
- This so-called 'emergency payment' aspect of the system has received inadequate explanation or scrutiny as yet, and is inherently dangerous and subject to expansion. It requires more legislative definition and limitation, and without that both cl 73 item 9 and cl 35, item 16 should be deleted.
- 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, is the aspect that does most to ensure that this will evolve into a national ID card. The new Bill has not lessened this danger in any respect.
- Which card-face data is machine readable (if any), by what means and by whom, should be defined in the Bill.
- The new Bill is a significant step backward from the previous Bill in the protection of card-face data against copying without consent and particularly routine copying.

- The new Bill contains inadequate obligations on the government to protect the security of chip content, and inadequate definition of who may access data on the chip or copy it. They need to be strengthened.

- Despite improvements to the provisions dealing with demands to produce a card, they are still too weak, and 'pseudo-voluntary production' will result in the access card becoming a national ID card.

- It is sufficiently unclear in law that individual public servants would be liable under the offence provisions in this Bill that an explicit provision that they are so liable is essential.

- While cl 99 is valuable in attempting to limit the use of ID numbers, it is inadequate in relation to the public sector, where an additional privacy principle similar to NPP 7 is needed.

- These provisions concerning access to the Register, which they add clarity to the legislation and some valuable limitations on uses and disclosures, also confirm that, as critics have claimed, they Register will be a 'honey pot' for Police and intelligence investigators. This increases the need for the content of the Register to be more limited than is proposed, particularly in relation to photographs.

- People whose cards (or information in them) are misused in any of the above ways should be able to seek compensation for any actions which would constitute a breach of the Act's criminal provisions, but should only need to establish the breach on the basis of a civil action burden of proof.

- There are also additional significant issues that the Bill should cover, such as chip capacity, and explicit provisions concerning individual access to their Register entries and logs.

The inappropriately open objectives of the Bill

The stated objects of the Act (cl 7) are to reduce complexity in accessing federal government benefits, reduce fraud concerning them, to improve access to emergency relief, but also in cl 7(1)(e) 'to permit access card owners to use their access cards for such other lawful purposes they choose'.

Somewhat inconsistently with this last object, the government's insistence that this is not an ID card is stated in cl 7(2): '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, and perhaps a basis for an argument that some Commonwealth action purporting to be pursuant to this legislation is *ultra vires*. It is just window-dressing.

The new cl 7(3) stating 'It is the intention of the Parliament that this Act should be construed, to the greatest extent consistent with the attainment of its objects, so as to limit interferences with the privacy of individuals' may be useful, though it is not obvious which sections would be open to a usefully restrictive interpretation.

Neither cl 7(2) or 7(3) can overcome the negative effects of cl 7(1)(e) and the expanded 'voluntary' uses of the card that it enshrines. Cl 7(3) is subject to it, and cl 7(2) must be

interpreted in a way that is consistent with it. Actions that are taken by government to facilitate individuals using their access cards for a myriad of new uses can and will be justified by cl 7(1)(e). It should be deleted. It is no proper function of this Bill to promote other unknown and undefined uses of the card, if the government is serious that it is not to become an ID card. There is a difference between accepting that people will make uses of a government facility beyond its intended purposes and enshrining such 'unplanned' uses as an objective of the Bill. This clause is the prime example of the hypocrisy that underlies this Bill.

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'). These provisions will have little effect on that trajectory. 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 (including by this deceptive Bill), and it will be dangerous to their interests.

The card will be named at inception the 'Health and Social Services Access Card' (cl 67(1). But if its purposes are so fixed and limited, why can the Minister change the name of the card at any time (cl 67(1)), and without Parliamentary scrutiny (cl 27(6)), or even any consultation with the Privacy Commissioner (cl 67(5))? A change of name will be able to reflect any expanded functions. For example, it could in future be re-named as the 'Australia Card'. The Minister should not be allowed to change the name of the card, this should require legislation.

The 'ownership' farce

'An individual owns his or her access card' proclaims cl 78. However, in relation to the plastic card (the chattel), the most obvious form of property, cl 80 provides 'Despite subsection 78(1), an individual cannot sell his or her access card, or otherwise transfer any part of his or her ownership of it.' It is an offence to do so (cl 136). In relation to the only other relevant form of property, cl 78 adds

> 'Subsection 78(1) does not give an individual ownership of any intellectual property or information that, at any time, is on the surface of, or in the chip in, the individual's access card that the individual would not otherwise have.'

The positive consequences of this purported ownership (the way in which the access card is property) is not explained by the government at all, except by the statement that cards are usually owned by the issuing party rather than the recipient (Exposure Draft EM, cl 78). It does however explain in detail the policies behind the two succeeding clauses which negate the only types of property which cl 78 might create. It is difficult to see that the purported 'ownership' here gives the card-holder any significant rights that they would not otherwise have.

The Bill's ostensible granting of 'ownership' in the card is still deceptive. It is a provision which insults the integrity of the Australian Parliament and should be deleted from the Bill.

The Register

To obtain a card, anyone who is eligible for a Commonwealth benefit (which is pretty much everyone over 18) must (in effect) apply to the Secretary of DHS for inclusion on the 'Register'(cl 19). They must provide particulars and supporting documents as decided by the Secretary, so that the Secretary is satisfied of their identity (cl 19, cl 22). The Privacy

Commissioner gets to consult and 'comment' on this massive exercise in personal data aggregation (cl 19(3)), 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), phone number(s) and 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, a flag identifying which participating agencies a person has a relationship with, and details of a person's death (cl 35). The Register will also include a unique identification number for each person.

Opportunities for content expansion (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. The Register itself is not a 'legislative instrument' (cl 33(6)) and nor are the Secretary's decisions concerning specific aspects of its contents concerning individuals. Ministerial directions to the Secretary as to how the Register should be established and maintained are legislative instruments (cl 33)[1].

The principal remaining problem is that cl 35 item 18 provides for inclusion of additional information in the Register 'if the Administration Rules require information relating to the individual to be in the Register'. Section 187 provides that the Administration Rules (ARs) may contain provisions dealing with other matters permitted by provisions of this Act to be dealt with in the Administration Rules. Such rules are made by the Minister (cl 182), after consultation with the Privacy Commissioner (cl 183).

Since cl 35 permits ARs to add new types of content to the Register, this potentially allows unlimited expansion of Register content. However, cl 182 makes ARs legislative instruments, and therefore disallowable[2]. As a result, expansion of the Register would have some Parliamentary oversight, but would not require new legislation. Parliamentary scrutiny is therefore possible, but only in the weaker sense of disallowance rather than requiring positive approval. However, given the width of the Bill's objects, this is too general a power to expand the Register. It should require new legislation. Clause 35 item 18 should be deleted.

Such an AR would also need to be *intra vires* the general purposes of the Act, but given the unjustifiably broad objects clause in cl 7(1)(e), it would be too easy for this to be satisfied, by any AR that seemed to facilitate how users 'chose' to use their cards. It is another reason for deleting cl 7(1)(e).

The uncertain position of POI data

The previous Bill gave the Secretary an astonishing power to include copies of any proof of identity documents in the Register (previous Bill cl 17(1), item 12), and such decisions were

---

[1] In the previous Bill, the Minister could determine to add 'other information' 'that is for the purposes of this Act', but must do so by legislative instrument (previous cl 17, item 17(b)).

[2] In the previous Bill, the same deficiency was present. The Minister could determine to add 'other information' 'that is for the purposes of this Act', but must do so by legislative instrument (previous Bill, cl 17, item 17(b)).

beyond Parliamentary scrutiny (cl 17(2)). This 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, was castigated by the Taskforce (2007a) as a broken undertaking[3]. The Register's potential as a 'honeypot' for ID fraud and privacy invasion was criticized on many occasions (eg Greenleaf, 2006, 2006a, 2007; APF 2007), with arguments that item 12 should be deleted from cl 17 entirely.

The new Bill is an improvement. It does not provide for POI data to be included in the Register, though the Secretary will still collect it. However, as discussed above, cl 35 item 18 provides for ARs to allow for inclusion of other information in the Register. POI could therefore still be included, but it would require a (disallowable) AR for this to occur. It would be difficult to argue that such inclusion was ultra vires, whether or not cl 7(2) was deleted. The dangers of an AR being used to expand the Register to include POI data reinforce the need for cl 35 item 18 to be entirely deleted from the Bill.

Excessive content – photos, contact and location data, and 'interim' IDs

The potential function creep described above is however, only a secondary danger. The main problem with the Register remains: it will constitutes an accumulation of personal information which is unprecedented in Australia.

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, so the Register will include the first national photo database. Second, it adds a national database of people's signatures. Third, phone numbers and email address are no longer included in the Register 'on request' as in the previous Bill, but whenever the Secretary holds them. The accumulation of the phone numbers and email addresses of virtually everyone in Australia has major telecommunications surveillance implications.

The collection together of photograph, signature and telecommunications contact information on most Australians create a system which creates a high security risk for identity fraud from unauthorized access, changes irrevocably the nature of police and intelligence surveillance because of these agencies' powers to access the Register (discussed later) and creates opportunities for future abuse by legislated changes to the system.

The so-called 'emergency' payments number

Another opportunity for function creep, unchanged from the previous Bill, is the provision for an 'Emergency payments number' to be included on the chip of a person's ID card (cl 73 item 9) and in their Register entry (cl 35, item 16). There is no further definition in the new Bill of how this will work, though it is described as operating as a debit number through which payments may be obtained by all eligible persons from ATMs ('it must conform to banking sector requirements) in the event of 'natural disasters and emergencies' (Fact Sheet: 'Emergency Payments').

The problem is that 'emergency' is nowhere defined in the Bill (though it has been defined in recent privacy legislation). This is therefore an open-ended mechanism by which the

---

[3] The Taskforce said 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.'

government can potentially limit the distribution of any type of welfare or other payment through only those outlets that it chooses to authorise to receive payments via the 'emergency' debit numbers. For example, the government has recently declared that there is a national emergency in the misuse of welfare payments to indigenous people. If this mechanism was in place, a government might be able to use it to limit how and where welfare funds could be distributed to them. This aspect of the system has received little scrutiny as yet. It requires more legislative definition and limitation, and without that both cl 73 item 9 and cl 35, item 16 should be deleted.

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 of the individual, 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 71, and cl 72 concerning optional information). All of this is also in the Register.

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, is the aspect that does most to ensure that this will evolve into a national ID card. The new Bill has not lessened this danger in any respect.

Expansion and control of card surface content

The only content on the card surface can be that which is specified in cl 71 (cl 70). 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 67(4)), without Parliamentary scrutiny (cl 67(6)), but with an added requirement to consult with the Privacy Commissioner (cl 67(5)). The 'form' 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.

No protection against copying of card face data

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.

Unlike the previous Bill, where there was some protection against copying of card-face data (previous cl 57)[4], this Bill contains no such protections. Any content on the face of the card can therefore be copied by anyone to whom the card is presented, whether in the public sector or the private sector. The card and its surface content are not 'protected records' (cl 89), except in relation to actions by agencies involved in the administration of the Act, so none of the confidentiality provisions in Part 5 will apply to anyone who obtains access to a card for other reasons. The only protections against such copying are the very limited ones provided by the law of breach of confidence, and the collection limitation rules in the NPPs and the IPPs. The IPPs relating the Commonwealth and some State public sectors do not even contain limitations on the collection and use of the ID number on the card.

As a result, there is a significant but difficult to quantify danger that an aggregation of people's personal details (including name, card number, photograph, signature, date of birth, and benefit-related information) may be routinely collected far more often than would be the case if the access card did not exist or (as we shall see later) if it was not so easy for organisations to ensure that individuals produced it on request.

The new Bill is a significant step backward from the previous Bill in the protection of card-face data against copying without consent and particularly routine copying.

The Card – in the chip

The Secretary must ensure, whenever the Secretary is able to change information in the chip (presumably including whenever a card is read by a DHS card reader) that the only information in the chip is that which is supposed to be there (cl 73).

Content of the chip

The chip will include everything that is on the surface of the card, other than the signature, plus a lot more information. It includes a person's 'legal name' and 'preferred name', photograph, access card number, card expiry date, information about benefit cards held, 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 74). Also included, but added since the previous Bill, are date of birth (optional), codes under

---

[4] In Greenleaf (2007) this was summarized as: '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.'

the International Classification of Diseases (for DVA white card holders), organ donor status, and a flag showing whether they have a relationship with a participating agency. Their sex and residential address are no longer included.

A potentially dangerous item on the chip is the designation on the chip of whether a person's POI is 'full' or 'interim', which is determined by the Secretary's discretionary power over the corresponding Register entry. 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). This is an aspect of the Bill to which rights of review should apply.

Function creep in the chip's content

The same danger of function creep is present with the chip as with the Register: cl 74 item 17 allows additional information to be added to the chip 'if the Administration Rules require information relating to the individual to be in the chip in the access card'. In combination with cl 187, this provides a mechanism for unlimited expansion of what can be in the chip[5]. As with the Register, the AR is a legislative instrument so Parliamentary disallowance is necessary for the chip's content to be expanded, but new legislation is not. Consultation with the Privacy Commissioner is also required.

It is unnecessarily dangerous that the range of personal information contained in the access card chip can expand without new legislation, so cl 74 item 17 should be deleted.

Has 'your area' of the chip disappeared?

The previous Bill asserted 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' (previous cl 33). It was further explained that (EM 2007 to previous Bill):

> '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.'

The complexities and difficulties of this approach were detailed by many, including the Taskforce's Discussion Paper on emergency and medical information (Taskforce 2007a), showing that these provisions were oversimplified and misleading (see Greenleaf 2007).

The provisions in cl 73 now seem exhaustive of information that can be on the chip at the outset, with no provision for 'user-generated content' or even 'doctor-generated content'. There is no current provision for storage of medical or financial information, other than references to organ donor status. 'Your area' of the chip, and with it former Minister Hockey's notion of an ID card as something akin to an IPOD (the IpoD Card?), seem to be dead. However, no obituary is found in the explanatory materials for the new Bill (Exposure Draft EM, 2007). The Fact Sheet: 'Protection of Privacy' does however state 'No financial information, medical records or tax file Numbers will be on the card, the chip or the Register'. This is consistent with what is apparently a major change in the new Bill for the better: the abandonment (at least for now) of plans to include a user-controlled 'your area' of the chip.

---

[5] Confirmed by Exposure Draft EM, cl 74.

As explained above, it is possible for the content of the chip to be expanded (subject to possible Parliamentary disallowance). It is therefore premature to declare 'your area' of the chip dead completely as yet. Like Monty Python's parrot, it may be 'just resting'.

Inadequate legislative requirements to protect chip content

The new Bill contains inadequate obligations on the government to protect the security of chip content, and inadequate definition of who may access data on the chip or copy it.

The only technical protection of chip content required *by the Bill* is that PIN protection is required for name, DOB and POI status on the chip (cl 77). However, the Fact Sheets (2007) claim that other forms of security will be provided, including for example:

- 'Only the Office of the Access Card and participating agencies will have the software capable of reading the photograph from the chip of the card.' (Fact Sheet: 'Photograph, Card Number and Signature')
- 'Information held on the chip … will be protected using advanced technology such as encryption and secure zones'. 'Security controls include: … the digital signing of all data on the card using Public Key Encryption technology' (Fact Sheet: 'Information Security').

These claims are a deceptive reassurance because the Bill does not require any of these protections. Criminal offences for unauthorised access to, or modification of, chip content (cl 97) only apply to 'restricted information', which is data held in the chip to which access is restricted by an access control system associated with a function of the chip (cl 97(5)). Nothing in the Bill requires such protection by an access control system, except for the very limited PIN protection required by cl 77.

The security measures claimed by the Fact Sheets may happen, and if the technical protections constitute an access control system, then cl 97 will apply to add legal sanctions against unauthorized access or modification of any data so protected. But there is no legislative guarantee that any of this will happen. At present, the Bill provides no way of determining which data are and are not protected by which security means, if any.

As the Bill stands, photos and other details on the chip are not *required* to be protected by any technical measures which would activate the cl 97 offence. There is therefore no legal protection against anyone accessing or copying these details from the chip, no matter who they are or what means they use to copy the data. In addition, the card and the chip are not 'protected records' (cl 89), so none of the confidentiality provisions in that Part will apply.

The new Bill does not contain any separate provisions against copying of data from the chip, a deficiency it shares with the previous Bill[6]. If the cl 97 offence does not apply, then only

---

[6] In Greenleaf (2007) this was summarized as '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 … As with all other offences in the Act, the Crown (Commonwealth, State and Territory agencies and their employees) are immune from prosecution under

the limited protections provided by the law of breach of confidence, or privacy principles, will apply.

This lacuna in the legislation opens the door for expanded uses by the private sector or the public sector to be facilitated by what data is and is not protected by which security means. Whatever security measures are or are not used is beyond legislative control. For example, there is nothing in the Bill to determine the answers to questions such as: Which data will be able to be read and copied 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?; When will chip content be able to be read remotely by 'contactless' means, and by whom? These are important questions, and the Bill should provide answers to them.

Access to the card - 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. This exacerbates the dangers of routine copying of card content, discussed above.

Card-holders are expressly entitled to use the card 'for any lawful purpose' (cl 81), 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.

Inadequate offences for requirements to produce

When is an agency or organisation (including a participating agency) prohibited from obtaining a person's card? A medical practitioner assessing a person's eligibility for a Commonwealth benefit, and a provider of goods or services assessing a person's eligibility for their provision on a concessional basis because of a benefit card (cl 131) can require a person to produce an access card.

Otherwise, it is an offence for anyone to require a person to produce an access card, or to make a statement which a person could 'reasonably understand' to require such production (cl 133). This is an improvement on the previous Bill which defined the offence in terms of whether the requirement was made in connection with the provision of a widely-defined list of benefits (previous cl 46), an approach criticised (Greenleaf 2007) because it would be simpler to prohibit production for 'any other purpose' than those expressly allowed[7]. This has now been addressed.

Despite this improvement four criticisms can be made of the likely effectiveness of these offences to achieve the government's professed 'major objective' 'that access cards are not to be used as national identity cards' (Exposure Draft EM, cl 131).

First, the broader criticism of these offences is that they can easily be side-stepped, simply be an organisation or agency refusing to accept successively proffered items of identification

---

cl 57. Most State and Territory governments are also not inhibited by information privacy laws binding them. It is hard to see how they can be restrained once a card is presented to them.'

[7] As stated in Greenleaf (2007): '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'.'

until a person 'voluntarily' produced their 'access card' in desperation. There does not have to be any uniform policy of refusing other IDs. A 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 133 on a criminal standard of proof, unless the organisation concerned was foolish. 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.

Second, this criticism is not effectively addressed by the infringement notice scheme added to the new Bill. Instead of prosecution for a breach, 'the Bill provides for a system of infringement notices to deal with less egregious cases of demanding an access card for identity purposes' (Exposure Draft EM, cl 131). The fine, if paid, is 20% of the maximum fine for the offence (cl 148(2)), which in the case of a breach of cl 133 is $2640 (24 x $110 penalty units, since cl 131 carries 120 penalty units). This approach, described as 'similar to a parking ticket' by a Department official at an access card briefing, runs the risk of trivialising the significance of breaches, as well as keeping their occurrence out of the spotlight of the criminal courts.

Third, both approaches based on enforcement at the discretion of the State are inadequate. The Bill omits any provision for civil compensation claims for improper demands for production of the card, as will be discussed below. The opportunity for individuals to directly seek significant compensation for breaches is needed to ensure that tardiness in enforcement by the State does not keep breaches buried.

Fourth, it is unclear whether improper requirements by governments for the production of a card could be prosecuted at all. 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)), apparently in accordance with normal Commonwealth drafting policy[8]. The question therefore becomes whether individual public servants in any jurisdiction can be prosecuted. The Commonwealth's assumption is that '…Crown immunity from criminal responsibility does not extend to Crown servants. An officer, servant or agent of the Commonwealth who commits an offence has no immunity from criminal responsibility: *Jacobsen v Rogers* (1995) 182 CLR 572 at 587'[9]. This assumption seems to be overly simplistic. In the later cases such as *Laing v Carroll* [2005] FCAFC 202, which concerned a provision with wording similar to cl 9(2), it was held that 'State employees, through whom a State acts, cannot be prosecuted'. If a court took this approach, it appears that any individual officers who breached cl 133 would also be immune from criminal proceeding. It is likely that a Court would refuse to exercise its discretion to even make a declaration that the Crown or its employees should

[8] Exposure Draft EM, cl 9, quoting *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*, Minister for Justice and Customs (February 2004)

[9] Exposure Draft EM, cl 9, quoting *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*, Minister for Justice and Customs (February 2004)

comply, given that they are immune from prosecution[10]. For example, in *Bropho v Western Australia* (1990) 171 CLR 1 (cited in *Jacobsen v Rogers*), the High Court said

> "if the question in issue is of the kind involved in the present case, namely, whether the employees of a governmental corporation engaged in commercial and developmental activities are bound by general provisions designed to safeguard places or objects whose preservation is of vital significance to a particular section of the community, the presumption against the applicability of general words to bind such employees will represent little more than the starting point of the ascertainment of the relevant legislative intent. Implicit in that is acceptance of the propositions that, notwithstanding the absence of express words, an Act may, when construed in context, disclose a legislative intent that one of its provisions will bind the Crown while others do not and that a disclosed legislative intent to bind the Crown may be qualified in that it may, for example, not apply directly to the Sovereign herself or to a Crown instrumentality itself as distinct from employees or agents. "

Rather than there being a clear rule that public servants are liable, as the High Court only describes a 'presumption against the applicability of general words to bind such employees' which 'will represent little more than the starting point of the ascertainment of the relevant legislative intent'. It seems that it depends on the circumstances of a particular case. One of the circumstances here is that other offences by individual Commonwealth officers are defined (cl 143 and 144), but they do not include wrongfully demanding a card. This would seem to increase the likelihood that a court would find that at least Commonwealth public servants were not liable to prosecution.

There is sufficient uncertainty here that, if the government is serious, as it claims to be, in wanting to prevent the access card becoming an ID card, it must include a provision that explicitly states that nothing in cl 9 prevents any Crown officer from being prosecuted for a breach of the Act. Otherwise, cardholders may be left even more defenceless against wrongful demands for production by the Crown, including by State and Territory government agencies.

Uses of a card, once produced

Even though an access card is not a 'protected record', information obtained from it by a 'regulated person' (essentially, those carrying out functions under the Act) becomes 'protected information' (cl 89), and Part 5 restricts the uses that can be made of it.

Otherwise, there are generally no restrictions on the purposes for which the information on an access card can be used, if a person (in both public and private sectors) can obtain access to the card, or the content of the chip. As discussed, there are no limits in the Bill on what can be copied from the card surface, and the question of who can access what information in the chip is left very uncertain. If access can be obtained to information on the chip, 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

---

[10] 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.

parties, some uses by employers, and so on. If a State agency obtains access, no privacy legislation will apply in some 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'.

Special protection for ID numbers

One exception is the strict liability offence for the use of the a person's access card number as an identifier by an organisation (public or private sector), or use or disclosure of the number (cl 99), provided (for a private sector organisations) this use would also breach NPP 7 concerning identifiers (cl 99(4)). This attempts to enforce against public sector bodies, by an offence, an obligation to which private sector bodies are liable by NPP 7. There should also be an amendment to the IPPs in the *Privacy Act* to add a similar principle, so that there is civil liability.

These protections will not, however, interfere with the 'voluntary' uses of the access card as an ID card: 'In addition, the Administration Rules will allow the access card number to be used or disclosed to the extent it is necessary to do so in circumstances where the access card has been offered as an identification document by the card holder' (Exposure Draft EM, cl 99).

Access to the Register – Enshrining the 'honeypot' for investigators

The previous version of the Bill was criticised for its failure to define which government agencies would be able to use their demand powers to obtain information from the Register, potentially on a mass scale. This Bill clarifies that access to and disclosure from the Register (or other 'protected information') is generally prohibited unless authorised by provisions in this Bill, and that such prohibition applies despite any contrary provisions in other previous or subsequent legislation (cl 116). This is a considerable improvement, recommended by submissions on the previous Bill.

Access to the Register is generally limited to access for the purposes of the Act (Part 5 Division 3, particularly cl 90 and 91). The Bill then sets out exceptions (Division 4). It makes explicit that Register information can be disclosed to any participating agency which is 'flagged' as having a relationship with a person (s101), which makes clear that the updating of Register information will find its way into the statutory data matching system.

The most contentious exceptions are those in favour of Police and intelligence agencies. Any 'senior' police officer (variously defined) can certify in writing that Register information is necessary for investigation or prosecution of a serious crime. A 'senior' intelligence officer, defined to include anyone authorised in writing by the heads of a security organisations, no matter how junior, merely has to certify in writing that information from the Register is connected with the functions of their agencies, and they can have whatever information they like. The claim by critics of the Register that its photos would be used to seek to identify persons of interest identified only by CCTV or other surveillance photos is purportedly addressed by the requirement that such certificates must identify persons of interest by their names. However, there are additional provisions where Police and intelligence agencies can require disclosure of information from the Register pursuant to a warrant. The legislative

provisions governing such search warrants do not require identification by name of the persons concerned but only such terms as 'evidential materials'.

These provisions tend to confirm that, as critics have claimed, they Register will be a 'honey pot' for Police and intelligence investigators, while at the same time limiting the extent to which it can be routinely included in the dragnet of Australia's proliferation of data matching systems.

Unjustifiable lack of civil remedies

The Bill omits any provision for civil compensation claims for improper demands for production of the card, or for any other misuse of the card or the information in it. The Bill's offences 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 'infringement notices' that have been added to the new Bill do nothing to remedy this.

The only remedy available at the initiative of a complainant would be a complaint to the Privacy Commissioner. It is not certain that a breach of this Bill's provisions would constitute a breach of the *Privacy Act*, though it is possible. The almost complete absence of Court decisions concerning the *Privacy Act* makes this completely speculative. 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, an ability to complain to the Commissioner is not a sufficient remedy.

People whose cards (or information in them) are misused in any of the above ways should be able to seek compensation for any actions which would constitute a breach of the Act's criminal provisions, but should only need to establish the breach on the basis of a civil action burden of proof. Individuals should have the option to proceed either by way of complaint to the Privacy Commissioner (where litigation costs are absent), or by going directly to a Court (with attendant risk of costs against).

If the government is as serious as it claims to be about preventing the access card from becoming a national ID card, it needs to give individuals an ability to protect themselves against its misuse.

Does this Bill cover everything it should?

There are issues that a comprehensive Bill needed to cover (Greenleaf, 2007), but this Bill still does not cover. For example, the Bill still does not guarantee whether individuals will be able to access what the Register says about them. It's easy to assume it will happen, but unless the Bill provides a mechanism, access will be ineffective. Reliance on the formalities of the FOI Act would be inappropriate and inadequate here. Similarly, will individuals know who has access to their records? The Bill does not guarantee that individuals can find out which agencies access their records on the Register, and the government previously refused to give a commitment that they could (SMH 8/2/07). This paper cannot be exhaustive on this question, but it is clear that the Bill is not yet comprehensive enough.

A fundamental question still unanswered by this legislation, is 'what will be the chip capacity'? Although this to some extent determines the possible additional uses of the card, it

is not specified by the Bill[11]. One of the most effective ways to limit function creep is for the Bill to limit the size of the chip, restricting it to a small enough size only to cover those functions that the government claims the scheme is intended to support. 'Crippled at birth' is the only safe approach to chip-based IDs – any other approach invites justified suspicion. The chip capacity should be defined in the legislation.

Conclusions - Still a national ID card, and should be rejected

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. Despite some improvements in this Bill, this 'voluntariness' can still be made illusory. 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.

The quarterly examinations I have made of this scheme since it was announced (Greenleaf, 2006, 2006a, 2007) 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 second attempt at a Bill changes my views. It still quacks like the dead duck of 1987. This Bill has tinkered with the capacity for function creep built in to all aspects of the system, limiting some and expanding others, but still leaving too many beyond Parliamentary control. It will lead to a national ID system despite its Big Lie that it is not one. Major improvements still need to be made to the Bill before it is a blueprint for a 'health and welfare' access card and nothing more than that.

References

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

Fact Sheets 2007 Australian Government Department of Human Services

Greenleaf, G. 2007 ' "Access All Areas": Function Creep Guaranteed in Australia's ID Card Bill (No. 1)' [2007] UNSWLRS 11 (on bepress at <http://law.bepress.com/unswwps/flrps/art11/>)

Greenleaf, G. 2006b 'Australia's Proposed ID Card: Still Quacking Like A Duck' *Computer Law & Security Report*, Vol. 23, 2007; [2007] UNSWLRS 1 (on Legal Scholarship Network at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=951358)

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>

[11] 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.'

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>