The Conjurer's New Card Trick and the Illusion of Privacy

A discussion of the privacy and transparency issues associated with the proposed Australian Government Health and Social Services Access Card

CAROLINE HART*

Introduction

On 7 February 2007, the *Human Services (Enhanced Service Delivery) Bill 2007* was introduced into the Federal Parliament by the Minister for Human Services. The purpose of the Bill was to introduce a Health and Social Services Access Card (the 'Access Card') by 2008[1] using smart card technology. Registration for the card was to be required by all Australian citizens seeking entitlement to health and social service benefits. The introduction of the Access Card would be within an Australian Government-controlled framework of interoperable smart cards. This structure may not necessarily have been accessed under the *Human Services (Enhanced Service Delivery) Bill 2007*, but it is certainly available for current and future government smartcard use.

The Bill, passed by the House of Representatives on 28 February, and then introduced into the Senate on the same day, was adjourned and later withdrawn that same day.

* BA/LLB (UQ), LLM (QUT), Solicitor (Qld), Lecturer (Law) at University of Southern Queensland.

[1] KPMG, Department of Human Services, Health & Social Services Smart Card Initiative Volume 1: Business Case Public Extract, Commonwealth of Australia, February 2006, at page 28 recommends a three and a half year timeframe for implementation: 18 months of planning, design and build; followed by a 24 month registration period, with start date in 2008. Registration process for the HSS system (KPMG, page 29) would be carried out in: Medicare offices (9.5 million expected); Centrelink officers (6.5 million expected).

The Access Card and the Register (the database that supports the Access Card) both have the potential to permanently erode the established rights of Australian citizens to information privacy currently secured by the *Privacy Act 1988* (Cth). This paper analyses the detrimental impact of the Access Card on privacy with respect to three concerns: the potential for function creep; that it is in all respects a quasi-identity card; and that it provides the opportunity for increased identity fraud and identity theft.

Structure of this paper

The structure of this paper is as follows: Part 1 provides an overview of the proposed Australian Government Health and Social Services Access Card (the 'Access Card') put forward in the *Human Services (Enhanced Service Delivery) Bill 2007*; Part 2 considers Australia's existing public sector privacy regime; Part 3 provides a brief insight into 'smart card technology'; Part 4 identifies and discusses the key legal issues associated with the proposed Access Card. Finally, Part 5 provides some recommendations to better protect the privacy of prospective users of the Access Card if the legislation were to be progressed by a future government.

Part 1 - Overview of the proposed Australian Government Health and Social Services Access Card and Register

This paper refers to and analyses the key documents that have been used to progress the policy and legislative implementation of the Health and Social Services Access Card, including the Business Case prepared by KPMG, the *Human Services (Enhanced Service Delivery) Bill 2007* ('the Bill'), and the accompanying Explanatory Memorandum to the Bill.[2]

Initiating the Health and Social Services Access Card and Register

In October 2005, the Australian Government asked the Federal Minister for Human Services to submit a business case for the introduction of a health and services smart card that would replace the current Medicare Card, veterans' health cards, and various Centrelink cards and vouchers, commencing as early as possible in 2007.[3]

[2] The terminology of the KPMG Business Case refers to 'the Access Card' and 'the SCRS Database'. This terminology of the Bill is that of 'the Access Card' and 'the Register'.

[3] Summary of the outcomes to be achieved are from the *KPMG Business Case*, at pages 10 to 12.

The Access Card Consumer and Privacy Taskforce was established by the (then) Minister for Human Services, the Hon Joe Hockey MP 'in order to facilitate a process of community consultation about the issues raised by the Government's Access Card and to open up additional lines of input to the Government's final decision making...'[4]

Why did the Australian Government seek to introduce the Access Card?

The Bill[5] provides that the objects of this Act are to reduce complexity of accessing Commonwealth benefits, including access for relief in emergency situations; to make this process more convenient, user-friendly and reliable; to reduce fraud on the Commonwealth with respect to benefits; and to permit Access Card owners to use their Access Cards for 'other lawful purposes they choose'. The Bill expressly provides that 'Access Cards are not to be used as, and do not become, national identity cards.'[6]

It is not within the scope of this paper to discuss the implications of all the objects of the Bill. This paper focuses on the objects of the capacity of the Bill to reduce fraud, and the likelihood of the Access Card becoming an identity card, despite the expressed intent of section 6. Part 4 analyses both objects in detail with reference to the Bill.

Will it be mandatory to have the Access Card?

Although it was stated[7] by the *KPMG Business Case* that registration for the Access Card will not be mandatory, and the Bill does not specifically address this issue, the reality is that in order to seek health and social security entitlements, it will become mandatory to register.

[4] Access Card Consumer & Privacy Taskforce, The Australian Government Health and Social Services Access Card, Discussion Paper Number 1, 15 June 2006, Available through the Department of Human Services Website, downloaded 9/08/06, at page 3.

[5] Human Services (Enhanced Service Delivery) Bill 2007, section 6.

[6] The Bill, section 6(2).

[7] KPMG, Business Case at page 15. KPMG outlined a number of 'significant problems' of a voluntary system, including, the continuation of a 'legacy system' and the negation of benefits linking to addressing fraud (KPMG, 14 – 15). Slipped in among the 'significant problems' was the 'great benefit of a uniform registration system' that would offer 'greater levels of certainty for government...'

The Bill links the requirement for registration, with entitlement to a broad range of health and social service benefits which means that most Australian citizens will need to register for the Access Card in order to be eligible for the entitlements. The figure for anticipated registration from the *KPMG Business Case* was that 'up to 16 million Australians'[8] will need to be registered for entitlement. The Bill operates as follows: Section 7 provides that the purposes of the Act are to facilitate the provision of benefits and services to members of the public from participating agencies. A 'participating agency'[9] includes the Department of Human Services, the Department of Veteran Affairs, Medicare Australia, Centrelink, Australian Hearing Services, and Health Services Australia Limited. In order to receive benefits or services from these services, the Access Card must be used, as required by Section 41, the Bill. Section 22 provides that to be eligible for an Access Card, a person must be registered on the Register.

Key components of the Human Services (Enhanced Services Delivery) Bill 2007

There are two key components to the Bill: the Register and the Access Card.

1. The Register

The Bill provides that registration requires a person to be eligible or qualified for a Commonwealth benefit, and not to already be registered.[10] Application is by written application in the form approved by the Secretary, and accompanied by 'such other specified information' that the Secretary determines is needed for the Secretary to be satisfied of the applicant's identity.

The Bill provides that once a person is registered, the Secretary must include on the Register the following information: a person's legal name; date of birth; citizenship or residency; indigenous status; sex; contact details, including residential address and postal address; benefit cards; registration status; details on the Access Card, if a person owns one; Department of Veteran Affairs information relating to pension; if a person was a prisoner of war; copies of the documents that were produced to prove identity and information about those documents if

[8] KPMG, Business Case at 3.

[9] The Bill, section 5, ' Definitions'.

[10] The Bill, section 12.

provided; details on the person's relationship with any of the participating agencies; date of death; and other information including 'other information that is determined by legislative instrument.'

The Explanatory Memorandum[11] states that: 'The Register will be separate from the databases maintained by the various delivery agencies such as Centrelink, Medicare Australia and the Department of Veterans' Affairs and the other Human Services agencies. There will be no centralised database holding all of an individual's information in one place. Existing agency records will remain with the relevant agency – where they are now.' Despite this, the content of the Register clearly contains information that was created by many of these agencies (and others) including 'Medicare number', details of citizenship, details of indigenous status, and details of benefit cards. It is likely that a person applying for registration would provide more information rather than less information, given the offences relating to applications for registration or Access Cards[12] in which a person commits an offence for omitting 'any matter or thing without which the statement is misleading'.

2. The Access Card

An applicant for the Access Card must be at least 18, [13] although an exemption from this can be obtained.[14] The applicant must be registered on the Register.[15] Application for an Access Card similarly requires completion of an approved form.

An applicant must accompany the form with such other specified information or documents that are needed for the Secretary to be satisfied of a person's identity. These provisions match the requirement for proof of identity documents and information required for registration.

Before an Access Card can be issued, an applicant must also attend an interview; have a photograph taken; provide their signature; and again the Secretary must be satisfied of the applicant's signature.[16] These three requirements are subject to exemption.[17] The provision provides that

[11] Explanatory Memorandum, 20.
[12] The Bill, sections 58 and 59.
[13] The Bill, section 22.
[14] The Bill, section 65.
[15] The Bill, section 22.
[16] The Bill, section s 24(1)(f).
[17] The Bill, section 65.

'other requirements determined by legislative instrument may need to be satisfied'. The chance for future legislative amendment is discussed in Part 4. The period of validity of the Access Card is 10 years.[18]

The information on the Access Card is contained in two places: the surface of the card;[19] and in the Commonwealth's area of the chip on the Access Card.[20]

Information on the surface of the Access Card

The Access Card must include the following information: legal name of card owner; Access Card number; expiry date; photograph; signature; date of birth. If the card owner chooses, information relating to the Department of Veteran Affairs information (including if the card owner was a prisoner of war) and details concerning blind disability support can be included on the surface.

Information in the Commonwealth's area of the chip in the Access Card

The microchip in the Access Card will contain the following information: card owner's legal name; date of birth; sex; residential address; photograph; signature; card number; expiry date; card PIN; benefit cards information; Medicare number; reciprocal Health Care Card number; emergency payment number (optional); registration status; Department of Veteran Affairs details (as provided in the Register); and statements required by legislation (no explanation is provided under the Explanatory Memorandum regarding these statements).

The Bill has not included the following information that was originally discussed in the *KPMG Business Case*: the 'concession and safety net status flags'; 'optional carer/legal custody status'; 'optional organ donor status'; or 'optional personal health details (allergies, drug alert notifications and chronic diseases)'.

Once issued, the successful applicant is held to 'own' their Access Card.[21] The concept of card ownership, is dealt with by the Bill, but not discussed in detail in this paper.

[18] The Bill, section 26.

[19] The Bill, section 30.

[20] The Bill, section 34.

[21] The Bill, section 37.

Who will have access to information on the card?[22]

The Bill[23] provides the Secretary with the power to appoint 'authorised persons' who, if acting for the 'purposes of this Act' will not be committing offences relating to the Access Card or Register. Appointments to be an 'authorised person' are: a Commonwealth officer in a participating agency; [24] a Commonwealth officer prescribed by the regulation; or an individual prescribed by the regulations.

How will the card be implemented?

Originally, the Governance and program implementation of the Access Card Project was[25] proposed to be by a single implementation unit to be established and called the 'HSS Smart Card Management Authority'.[26] This authority was to include a board and a stakeholder advisory body comprised as follows: Secretary of Department of Human Services; CEOs of Medicare and Centreline; Secretaries of agencies including: Prime Minister and Cabinet; Finance and Administration; Health and Ageing; Attorney General's Department; Department of Family, Community Services and Indigenous Affairs; Federal Privacy Commissioner. Also, an external firm (program management) to support the implementation of the project; and a stakeholder advisory body to report directly to the Minister and chaired independently. The role will be to co-ordinate stakeholder advice; oversight of implementation and coordination; advise on business rules, with privacy considerations; advise on communication, education and training; advise and make recommendations on any proposed expansion to functionality and scope.'[27]

The Bill has not implemented this Authority, instead, implementation is carried by the Minister (of the Department of Human Services), and the Secretary. The Secretary carries responsibility for the establishment and maintenance of the Register, and for the issuance of the Access Cards. The Bill[28] also provides for the 'administration of this Act to [be in]

[22] KPMG, Business Case at 44 – 45.

[23] The Bill, s 72.

[24] Defined at s 5, the Bill to mean: the Department (Human Services), the DVA, the CEO of Medicare Australia, the CEO of Centrelink, Australian Hearing Services, Health Services Australia Limited.

[25] KPMG, Business Case at 30, 31.

[26] It is referred to by this name for the purpose of the Business Case.

[27] *KPMG,* Business Case at 30, 31.

[28] The Bill, section 8.

accord with Australian Government policy'. The Bill allows the Minister, in consultation with the DVA Minister, to prepare a written statement of the policy of the Australian Government in relation to the administration of the Act, of which a copy may be given to the respective secretaries, and the statement must be laid before Parliament. If the Minister gives a copy to the secretary, then regard must be had to the statement in exercising powers and performing functions under the Act. However, the Bill declares[29] that such a statement is not a legislative instrument. The Explanatory Memorandum[30] offers only the following assistance in interpreting the implications of this section; that 'the provision is intended to allow the Minister to provide general high level guidance to the Secretary... about matters relevant to the administration of the Bill.'

This method of administration is certainly narrower and less inclusive of the broader range of interests and points of view than the initial proposal of the 'HSS Smart Card Management Authority'.

Part 2 – Australia's existing privacy regime with particular reference to provision of health and social services

The proposed Access Card will be introduced into a privacy regime predominantly established by the *Privacy Act 1988* (Cth). The Bill also provides a number of mechanisms through which information privacy may be protected.

1. The Privacy Act 1988 (Cth)

The Commonwealth *Privacy Act 1988* reflects the Australian Government's response to the international community's recognition of privacy. The Act acknowledges the *International Covenant on Civil and Political Rights*, Article 17 regarding the right to privacy; and the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The Australian Government version of the Guidelines is provided in eleven Information Privacy Principles[31] that relate only to the protection of privacy by government agencies. In 2000, the *Privacy*

[29] The Bill, section 8(6).

[30] Explanatory Memorandum, at 16.

[31] The Act protects personal information privacy through the establishment of eleven Information Privacy Principles[31] that are outlined in the *Privacy Act 1988* s 14.

Act 1988 was extended to cover (with exceptions) the private sector, achieved by the *Privacy Amendment (Private Sector) Act 2000.* The *Privacy Act 1988 (Cth)* has limited application[32] to specified Commonwealth agencies and certain private sector organisations;[33] and does not apply to the States or Territories.[34]

The Act deals only with the protection of 'personal information privacy', defined[35] as 'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.' This definition is sufficiently broad to cover personal information that forms part of a database and also personal information that is stored on a smart card, due to the wording 'whether recorded in a material form not'.[36]

Under the *Privacy Act*, the Access Card and Register would have been bound by the eleven Information Privacy Principles. The Information Privacy Principles ('IPPs') relate to collection and use of data (IPPs 1, 2, 3, 9, 10 and 11); storage and security of data (IPPs 4, 5 and 6); and accuracy of data (IPPs 7 and 8).
Part 4 analyses how the Australian Government's Access Card and Register would have breached its own existing privacy regime with respect to the principles relating to collection, use, disclosure and security

[32] Initially, the Act required only Commonwealth government agencies to comply with the eleven Information Privacy Principles. An additional amendment to the Act made by the *Privacy Amendment (Private Sector) Act 2000 (Cth)* has now extended the scope of the Act to include compliance by certain private sector organisations to ten National Privacy Principles, which are provided for in Schedule 3 of the Act.

[33] Additional exemptions from application of the Act by both Commonwealth Government agencies and private sector organisations are provided under section 7B.

[34] New South Wales has the *Privacy and Personal Information Protection Act 1998* which makes provisions for Information Privacy Principles (Part 2); Privacy codes of practices and management plans (Part 3); Privacy Commissioner (Part 4); and a Privacy Advisory Committee (Part 7). Victoria has the *Information Privacy Act 2000* which makes provision for: Information Privacy Principles (Part 3); Codes of practice (Part 4); and a Privacy Commissioner (Part 7). The Australian Capital Territory has the *Information Privacy Act 2000* and the Northern Territory has the *Information Act 2004.* Tasmania has the *Personal Information Protection Act 2004.*

[35] Section 6, *Privacy Act 1988.*

[36] The Australian Law Reform Commission, *Privacy Review, Issues Paper*, 2006 at pages 545 has raised the definition of 'personal information' and 'sensitive information' as items for review, particularly with new developments in technology that may make the definitions incomplete.

and storage of personal information.[37] The prospect of breaches of information privacy is heightened by the policy direction the Australian Government intends to adopt in its planned future use of smart card technology, not just with respect to health and social security entitlements, but by creating interoperability with smart cards used by all levels of government.

2. Protection of information privacy offered under the Bill

The Bill offers some protection of information privacy; however analysis will show that this protection is flawed. The protection offered under the Bill includes the following: Requirement for consultation with the Privacy Commissioner; limitations on collection of information; limitations on use of information; and offence provisions related to use of the Access Card.

(i) Input from the Federal Privacy Commissioner

The processes for registration on the Register and issuance of the Access Card allow only for a very narrow role for the Privacy Commissioner, in which consultation by the Privacy Commissioner is limited to commenting on the respective forms. Failure to take into account any comments by the Privacy commissioner will not however affect the validity of the approval forms.[38] Further, the consultative role of the Privacy Commissioner does not extend to any additional documentation that the Secretary has the power to require for the purposed of assessing an application.[39] Neither is the Privacy Commissioner consulted on matters that relate to the Secretary's request for 'additional information or specified additional document'[40] needed to satisfy eligibility or proof of identity.

There are a number of opportunities throughout the Bill for which consultation with the Privacy Commissioner might be valuable, most notably, section 66 in which the Minister has the power to determine

[37] If the Australian Government sought to contract out various aspects of the Access Card which resulted in an 'organisation' dealing with a prospective Access Cardholder's 'personal information' (or 'sensitive information'), then the National Privacy Principles (Schedule 3) may have application. This paper, however, does not cover an analysis of the Access Card under that circumstance.

[38] The Bill, ss13, 23.

[39] The Bill, ss 13(4), 23(4).

[40] The Bill ss 17, 34.

guidelines for decisions about identity.[41] It is noted, however that that the guidelines must be made by legislative instrument which will allow scrutiny by Parliament. The Federal Privacy Commissioner would have the advantage of offering expert advice on matters as they develop under the Bill.

(ii) Collection of information – limits on information that can be contained on the Register and on the Access Card.

The Bill provides a statutory limitation on the information that can be contained on the Register[42] and on the Access Card (on the surface,[43] and on the microchip).[44] However, the information that is listed as required to be provided on the Register[45] and on the microchip of the Access Card[46] is extensive, and includes personal information that has been collected for purposes not related to either health or social security purposes, for example personal information relating to citizenship and residency; and other identity documents. The Register also requires a person to provide 'sensitive information' relating to their indigenous status and disabilities.

Given the statutory breadth of information required, the legislative limitation appears ineffective as a means of minimising information on the Register and Access Card. The only express limitation regarding information on the Register and Access Card relates to if an applicant is included in the National Witness Protection Program.[47]

The Register is expressly declared not to be 'a legislative instrument',[48] as are determinations made by the Secretary concerning information to be provided regarding the Register and Access Card are expressly held not to be a legislative instrument.[49] The Explanatory Memorandum[50] provides that the Register and Access Card are administrative in character and that this is merely declaratory of that legal position. This may have

41 The identity guidelines are relevant for decisions under section 13(a)(b)(i) and 13(4)(b) that relate to applying for registration; section 14(c) that relates to registration; section 23(2)(b)(i) and section 23(4)(b) that relate to applying for an Access Card; and section 24(1)(f) relating to the issue of an Access Card.

42 The Bill, s 20.

43 The Bill, s 32.

44 The Bill, s 36.

45 The Bill, s 17, 19.

46 The Bill, s 34.

47 The Bill, ss 18(1), 35 respectively.

48 The Bill, ss 16.

49 The Bill, ss 17(2) and 34(2) respectively.

50 Explanatory Memorandum at 20, 38.

the effect of minimising scrutiny of Parliament over the content of the Register.

Under both sections providing for information that must be provided,[51] the Minister may determine by legislative instrument that other information is required for the purposes of the Act. Although this means that possible expansions of information will require an amendment through Parliament, it also provides for expansions without the expert oversight initially proposed by the HSS Smart Card Management Authority.

(iii) Use of information

The Bill provides for limits on the use of the Access Card in the following way. A person to whom the card is issued may use the card for any lawful purposes they choose.[52] Commonwealth officers in 'participating agencies' may only use an Access Card for purposes of the Bill or with the owner's consent.[53] Consent in this context is not defined as requiring consent to be in writing, or to be 'informed consent'. The Explanatory Memorandum[54] provide that '[t]he effect of the clause is to ensure that such officers are limited to using the Access Card to facilitate the provision of relevant benefits, services, programs and facilities.' By comparison, there is no companion section that expressly protects the use of information on the Register from 'use' by participating agencies, in the same way that section 40 seeks to protect use of the Access Card.

4. Security and storage of the information

The Bill does not provide any express provisions relating to the quality of security and protection of information stored on either the Register or the microchip of the Access Card. Instead the Bill provides for a series of offences that can be brought directly against persons who deal with Access Cards, including Commonwealth officers. However there is no express responsibility or duty upon the Secretary, or Minister to ensure the security and storage of the information on the Register and Access Card is of a particular standard.

[51] The Bill, ss 17, 34, at each Item 17(b).

[52] The Bill, s 40.

[53] The Bill, s41.

[54] Explanatory Memorandum, at 41.

Part 3 – Brief outline of smart card technology and Australian Government *Smartcard Framework* for use of smart card technology

3.1 About smart card technology

The proposed Australian Government's Access Card will use smart card technology. The 'form' of the Access Card is to be determined by the Minister.[55] The Explanatory Memorandum[56] provides that 'the new Access Card will be a smartcard... [i]t will contain an embedded microchip which will store information in a secure and safe manner.' The Bill (at section 27) has been 'drafted in a way which will not prevent the application of future technology which may be developed and which may provide additional security benefits to the card.'[57]

Smart cards have been described in a 1995 report of the New South Wales Privacy Commission as being:

> ...a plastic card, usually about the same size as a magnetic strip card that has electronic logic to store data and in some case a microprocessor that can process data. Both of these types of cards can be in the form of a contact or contactless card. A contact card has small metal contacts imbedded in it which when inserted into a smart card reader, transmits powers to the card and allows data to be transferred to or from the card...

The smart card chip is capable of being compartmentalized into 'open working, secret and super secret'.[58] For example, the open compartment of the chip can contain details of the cardholder's name and address, which can be accessed by anyone but not overwritten. The working component can contain information about the cardholder such as their blood type. The secret compartment can be accessed only the cardholder using a PIN. Finally, the super secret part contains the programs 'placed there by the manufacturer and/or the issuer of the card... and can only be

[55] The Bill, s 27(4).

[56] Explanatory Memorandum, at 29.

[57] Explanatory Memorandum, at page 29.

[58] Federal Privacy Commissioner, *Smart cards: Implications for privacy*, December 1995. Information Paper No. 4, at 7.

accessed by special codes usually only known by the chip manufacturer.'[59]

Smart cards offer true multi-functionality. Their 'storage and processing capacities are impressive, and it is not unusual to find a smart card that is capable of performing up to fifty different functions.'[60]

Given the Access Card's capacity for personal information storage and access, it may be considered an 'efficient policy decision' to add additional components to the Access Card, once it has been established. The Bill provides[61] that 'other information that is determined, by legislative instrument, by the Minister and that is for the purposes of this Act', may also be included in the Commonwealth's area of the chip in the Access Card. The Australian Government's policy on smart cards establishes the requirement of 'interoperability' between all current and future smart card projects (discussed in detail in Part 3.2). The Australian Government's policy of 'interoperability' is an indication that the Access Card may become the platform upon which other government (and possibly commercial) information storage and retrieval functions will be housed. Ownership of the Access Card is statutorily provided to the cardholder, [62] allowing the card owner to use their Access Card 'for any lawful purpose'.[63] It is possible for a commercial operator to offer other services that use the non-Commonwealth part of the microchip.

The Australian Law Reform Commission's *Review of Privacy, Issues Paper, 2006* stated[64] that smart card technology raises a number of privacy concerns. These concerns include: the lack of anonymity when making a smart card transaction; the ability to accumulate vast amounts of information about the activities of their users; and the ability to generate profiles based on this information.

The Access Card will be used by a number of 'participating agencies'. Without proper accountabilities, it will be difficult to determine

[59] Federal Privacy Commissioner, *Smart cards: Implications for privacy*, December 1995 Information Paper No. 4, at 7

[60] The Privacy Committee of New South Wales, *Smart Cards: Brother's Little Helpers*, Report, No. 66, August 1995.

[61] The Bill, section 34(1), Item 17.

[62] The Bill, s 37.

[63] The Bill, s 40.

[64] Australian Law Reform Commission, *Review of Privacy, Issues Paper*, Commonwealth of Australia, 2006, at 521.

responsibility for any breaches of privacy relating to it. The existing privacy regime in Australia does not specifically address smartcard concerns. The Council of Europe[65] has introduced *Guiding Principles for the Protection of Personal Data with Regard to Smart Cards* that 'sets out 11 principles to be taken into account by those who issue smart cards, as well as other participants in smart card systems, such as project designers and managers.'[66]

The *Privacy Act 1988 (Cth)* does not specifically address smart cards and may need to be amended to address the privacy implications associated with their use. The Australian Government has failed to progress any legislative framework that will afford protection to privacy in a 'smart card environment'. The Bill does provide for a number of offences relating to the Access Card, however these offences relate directly to individuals (including Commonwealth officers) who, for example, deal with an Access Card contrary to the Bill. The Bill provides no legislative framework for accountability or audit processes, or associated enforcement mechanisms that secure smartcard protections as a government responsibility. Instead, the Bill deals with these issues only at the individual officer level.

3.2 Australian Government's *Smartcard Framework*

The introduction of the Access smart card will fit within an Australian Government policy of use of smart cards, as outlined in the *Australian Government Smartcard Framework, Responsive Government A New Service Agenda.*[67] This is important because its policy of interoperability

[65] The Council of Europe introduced *Guiding Principles for the Protection of Personal Data with Regard to Smart Cards*, in 2004. Further references to the Principles are at page 522, Australian Law Reform Commission, *Review of Privacy, Issues Paper*, 2006.

[66] Australian Law Reform Commission, *Review of Privacy, Issues Paper*, Commonwealth of Australia, 2006, at 522.

[67] The set of documents is established by the Australian Government Information Management Office (AGIMO), June 2006 (the '*Smartcard Framework* '). Part B is the *Smartcard Handbook* in which an overview of smartcard technology in plain-English is explained. Part C is the *Standards and Model Specification* which explains the technical, business, functional and architectural aspects of smartcards and interoperability are dealt with. Part B is the *Implementation Guideline* in which the development of business cases for deploying smartcards and guidance for project management are explained (*Smartcard Framework*, A, p5). The vision of the Australian Government for the use of smartcards is that 'smartcards will become steadily more important in Australia.' The *Smartcard Framework* is intended 'to facilitate clear thinking about implementation issues... to help agencies understand the

of smart card application provides the context for the operation of the Access Card. The Australian Government is clearly anticipating (not necessarily at the point of passage of this particular Bill, but at some point), the development of a network of linked smart cards potentially through all levels of government, and out into commercial organisations. This 'interoperability' is clearly in breach of the existing privacy protections of the *Privacy Act 1988*.

The *Smartcard Framework* is 'intended to inform and guide adoption of a uniform smart card technology platform for all levels of government in Australia. The intention of the *Smartcard Framework* is to foster common interoperable[68] technologies. It provides an opportunity for establishing a platform for future interoperability and to build in extensibility.[69] The goals of the *Smartcard Framework* include delivering 'consistency of smart card deployments within the Australian Government and promote national alliance and interoperability' and to accommodate the 'development of smart card applications (single or multiple) matched to business requirements.'[70]

Part 4 – Three key legal issues associated with the Bill

This paper focuses on three key legal issues: Firstly, the potential for function creep regarding both the Access Card and the Register; secondly, the use of the Access Card as a quasi-identity card; and thirdly, the increased chance of identity fraud particularly with respect to the Register.

4.1 Function creep

The Access Card and the Register both have enormous capacities to store information and to link databases; there is the chance that the original

business case for smartcards, and to promote standardisation and uniformity for the shared benefit of all government agencies.' (*Smartcard Framework,* A at 8).

68 The *Smartcard Framework* defines 'interoperability' as being 'the ability to transfer and use information in a uniform and efficient manner across multiple organisations and information technology systems. It underpins the level of benefits accruing to enterprises, government and the wider economy through e-commerce.' This definition is taken from the *Smartcard Framework,* A page 11, 'What is the Interoperability Technical *Smartcard Framework?*' Australian Government Interoperability *Smartcard Framework*,Version 2, found at <www.agimo.gov.au/publications/2005/04/agtifv2/what_is>.

69 *Smartcard Framework* , at ii.

70 *Smartcard Framework* , at A9.

function or purpose for which the Access Card was introduced may, by a series of legislative amendments be used for other purposes or functions that were not intended. Although there are some legislative provisions in the Bill with the intention that function creep be (at least initially) limited, there is still the capacity for function creep.

This paper firstly defines the term 'function creep', secondly identifies if there is the potential for function creep with the Access Card and Register; thirdly discusses why function creep may be an occurrence that as a society we need to be cautious of, and finally proposes how function creep can be prevented, or at best minimised.

What is 'function creep'?

The Access Card Consumer and Privacy Taskforce in its *Discussion Paper Number 1* define[71] 'function creep', as:

> *...the way in which new systems, which are introduced for one specific or stated purpose, evolve or morph over time to serve quite different purposes and usages.* For example, driver's licences were originally introduced to do nothing more than to indicate that a certain person was permitted to be in control of a certain type of motor vehicle – nothing more. Today the driver's licence has evolved into something entirely different and is used for a variety of purposes which have nothing to do with motor vehicles. In many cases, it has assumed incrementally many of the characteristics of a comprehensive identity card. [this article's author's emphasis].

Comments in response to the *UK Identity Cards Act 2006,* have remarked that with respect to function creep, 'security features, such as subject-privacy guarantees, are immensely difficult, if not impossible, to retrofit.'[72]

Is there potential for 'function creep' with the Access Card?

There is an inevitability that function creep will occur as evidenced in the provisions of the Bill, the capacity to store proof of identity documents, and in the Australian Government's *Smartcard Framework.*

[71] *Smartcard Framework*, at 22.

[72] *Entitlement cards and identity fraud, Id* Card Response, Stand, January 2003, <http://www.stand.org.uk/IdCardResponse.html,>, at 19.

1. Provisions of the Bill

The Bill itself provides an indication that the structure it proposes for the Access Card and Register may be open to subsequent amendment and expansion. This is evident in the stated purposes of the Act; the objects of the Act; and the ability to require further information.

The purpose of the Act

The Bill[73], states that '[t]he purposes of this Act are to facilitate the provision of benefits, services, programs or facilities to some or all members of the public (whether under a Commonwealth law or otherwise), where that provision involves a participating agency.'

There are three ways in which the purpose of the Act can be expanded through an amendment that may not overtly appear to be an expansion of purpose. Firstly, there is no express limitation on the type or kind of 'benefits, services, program or facilities' to which the Bill relates. An amendment to include other 'benefits' would necessarily expand the Bill's ambit and function. Secondly, that such benefits may be provided under a 'Commonwealth law or otherwise', potentially creates the opportunity to include non-Commonwealth benefits. Might this include state or local government benefits? There is no limiting information either within the Bill or the Explanatory Memorandum.

Finally, the appearance of a limitation on the purpose is to be found at the end of the purpose provision through the involvement of 'a participating agency'. The definition of a 'participating agency' means the department; the DVA; Medicare; Centrelink; Australian Hearing Services; and Health Services Australia Limited. An amendment to either this definition to include an additional department, agency or service automatically expands the breadth of the purpose of the Act. Alternatively, it is possible to administratively expand the portfolio of 'the department' to encompass other purposes. The Bill[74] provides for legislative amendments to enable additional information to be required as part of the application processes for the Register and the Access Card. If the list of 'participating agencies' were to be expanded, then the respective sections above can be amended to support the collection of additional information required.

[73] The Bill, s 7.

[74] The Bill, ss17(1) Item 17, 34(1) Item 17.

The objects of the Act

The final object of the Act (coupled with other provisions) foreshadows the inclusion of commercial functions being included in the Access Card. The first four objects of the Act deal with reducing complexity, improving convenience; reducing fraud; and improving access. The final object relates to permitting 'Access Card owners to use their Access Cards for such other lawful purposes they choose'.[75] Vesting ownership of the Access Card in the cardholder,[76] and permitting use of the card for all lawful purposes, [77] provides the foundation for the Australian Government to allow the card to be used for other purposes including identification purposes or for the non-Commonwealth part of the microchip to be utilised for commercial purposes.

Opportunities for data-matching

The Taskforce is similarly concerned about the potential for function creep; in its *Discussion Paper* it is noted that, 'Although the Secure Customer Registration Service [the Register] will be established separate from the databases administered by participating agencies, its existence may place greater pressures on Government to expand data-matching exercises.' [78]

As the Australian Law Reform Commission's *Review of Privacy, Issues Paper*[79] notes data-matching:

> is currently conducted regularly in Australia, particularly by government agencies.[80] Data-matching can be conducted for a number of purposes, including detecting errors and illegal behaviour, to locate individuals, to ascertain whether a particular individual is eligible to receive a benefit and to facilitate debt collection.

[75] The Bill, section 6(e).

[76] The Bill, section 37.

[77] The Bill, section 40.

[78] Access Card Consumer & Privacy Taskforce, *The Australian Government Health and Social Services Access Card, Discussion Paper Number 1*, at page 22.

[79] Australian Law Reform Commission, *Privacy Review, Issues Paper*, 2006, at page 534 to 537.

[80] ibid, quoting R Clarke, 'Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism' (1995) 4 *Information Infrastructure and Policy* 29, 30.

The reasons may be laudable, however the privacy implications may long term, be negative.

The Federal Office of the Privacy Commissioner released a detailed report[81] on the handling of *Medicare* and the *Pharmaceutical Benefits Scheme* claims information which was released in August 2006. In this report it was stated that it was a 'statutory requirement that ... the Guideline [required] the separation of Medicare and PBS claims information.' The report highlighted the privacy implications for combining two databases dealing with Medicare claims and pharmaceutical benefit claims. The combination of the two databases has the potential to create a detailed profile of an individual relating to highly sensitive health information.

The *Medicare/Pharmaceutical Benefits Scheme* claims information database is one example of a database which, for privacy reasons, requires that information within a single portfolio must be kept separately. An audit (including reviews and updates) of databases may need to be undertaken to ensure that the combination of databases within (or without) a portfolio or department may need to be kept separately to avoid privacy implications. The pressure of ensuring 'efficiencies' may lead the Australian Government to (in the future) combine such databases.

The Bill requires that information ('as is determined by the Secretary') about a PBS Entitlement Card and PBS Safety Net Concession cards are included on both the Register and on the Commonwealth part of the microchip.[82] There are no express statutory provisions limiting the use and disclosure of that information such that might be expected following the Federal Privacy Commissioner's report[83] on the handling of *Medicare* and the *Pharmaceutical Benefits Scheme.*

2. Storing proof of identity documents

Proof of identity documents will be scanned into, and stored by the Register as described. This requirement will breach IPP 1, requiring information collected to be directly related to that purpose, and IPP9, that

[81] Report of the Privacy Commissioner's *Review of the Privacy Guidelines for the Handling of Medicare and PBS claims information*, August 2006, at 27.

[82] The Bill, sections 17 Item 7, and 34 Item 10, respectively.

[83] Report of the Privacy Commissioner's *Review of the Privacy Guidelines for the Handling of Medicare and PBS claims information*, August 2006, at 27.

information obtained for a particular purpose cannot be used for another purpose, without consent. This series of breaches will occur because documents used for proof of identity, such as driver licence, or passport, relate to information required for another purpose, that is, for the purpose of driving a vehicle, and for the purpose of entry into, and exit from Australia.

Once the information is scanned and stored, then access to this broader information, that is unrelated to information necessary to obtain Access Card related services can be used in breach of IPP 10, or disclosed in breach of IPP11.

A more fundamental question is why is the proof of identity required of such a high standard? The Australian Government in providing entitlements need only know that the person is duly entitled, and that there remains continuity in the identity of the person they are dealing with.

3. The Smartcard Framework

The *Smartcard Framework* indicates a planned network of 'infrastructure' in the form of smart cards into which government at all levels will be linked. Already, the *Smartcard Framework* has anticipated the Queensland Government's proposed 'New Queensland Driver Licence' project in which all licensed road users' information (including personal information, road traffic information, criminal records) will be linked into the Australian Government's *Smartcard Framework.*

The combination of the possibility for extended functionality permissible by the Bill that may allow extensive public sector and private sector participation; the capacity of the Register to store and retrieve documentation beyond health and social service related personal information; and the proposed use of interoperable technologies necessarily leads to the conclusion that the Access Card will, if implemented, be used at some point in time for many more purposes than it was originally intended.

Is 'function creep' a bad thing?

Daniel Solove in '*A Taxonomy of Privacy*'[84] discusses the issues of the ability of government to seek personal information and to maintain it on databases. He asks: 'What is the concern? The data was already in the record systems of government agencies. Why is it a problem for the government to combine it into one gigantic database?'

> The problem is one that I have called 'aggregation'...Aggregation is the gathering together of information about a person. A piece of information here or there is not very telling. But when combined together, pieces of data begin to form a portrait of a person. The whole becomes greater than the parts. This occurs because combining information creates synergies. When analysed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected.

The implications of this for the Access Card are that it is possible that sensitive information is capable of becoming apparent through the 'aggregation' of expanding amounts of personal information through the Register. In fact, the Bill does not address the concept of 'sensitive information' either through its definitions or via any means of protecting this information. It compulsorily requires information that directly relates to sensitive information (for example, indigenous information, health information), but does not require a standard for protecting that information.

The Australian Privacy Foundation[85] in its submission asserts that:

> Administration of health benefits unavoidably involves information relating to health care delivered, much of which is highly sensitive, it is for this reason that health administration information has been subject to specific privacy rules designed in part to quarantine it from other areas of public administration.

Further, the importance of 'function creep' becomes heightened as Solove comments:[86]

[84] Solove DJ, 'A Taxonomy of Privacy', 154 University of Pennsylvania Law Review, (3), January 2006, at 505.

[85] Australian Privacy Foundation, *Response to the Taskforce Discussion Paper No. 1*, at 13.

[86] Solove, above note 84, at 506.

> ...aggregation's power and scope are different in the Information Age: the data gathered about people is significantly more extensive, the process of combining it is much easier, and the computer technologies to analyse it are more sophisticated and powerful.

In terms of the Access Card, coupled with the Australian Government's *Smartcard Framework,* the capacity to aggregate information (not just personal information, but also cross-referenced information) from all levels of government and possibly commercial organisations becomes a possibility. Will the legislative safeguards of the *Privacy Act 1988* (Cth) that limit collection, use and disclosure be effective? These safeguards will not occur at the state or local level where the Commonwealth *Privacy Act 1988* does not apply. In states where privacy is legislated for[87] then additional protections will be available. In states such as Queensland reliance for protection is limited to a mere administrative guideline, *Information Standard 42*.[88]

Can function creep be prevented, and if so how?

The Taskforce *Discussion Paper* recommends[89] that function creep may be kept in check by 'specifying the exact purposes for which the Access Card is to be introduced...equally to specify the purposes for which it cannot be used...'[90] The Bill has not implemented the latter recommendation.

The Federal Privacy Commissioner in 1995 outlined guidelines[91] on how the privacy principles should be incorporated into smart card projects: [92]

[87] New South Wales has the *Privacy and Personal Information Protection Act 1998* which makes provisions for Information Privacy Principles (Part 2); Privacy codes of practices and management plans (Part 3); Privacy Commissioner (Part 4); and a Privacy Advisory Committee (Part 7). Victoria has the *Information Privacy Act 2000* which makes provision for: Information Privacy Principles (Part 3); Codes of practice (Part 4); and a Privacy Commissioner (Part 7). The Australian Capital Territory has the *Information Privacy Act 2000* and the Northern Territory has the *Information Act 2004*. Tasmania has the *Personal Information Protection Act 2004.*

[88] Queensland Government Information Architecture, *Information Standard 42, Information Privacy Guidelines*, V1.00.00.

[89] Access Card Consumer & Privacy Taskforce, *The Australian Government Health and Social Services Access Card, Discussion Paper Number 1*Taskforce, at page 22.

[90] Ibid, at page 22.

[91] This approach is consistent with the data protection laws that have been developed from the OECD Guidelines on Transborder flows of personal data, and expressed in academic journals, including, Donna Bain's Article: *Smart cards: a federal privacy perspective* (outlining the Australian Privacy Commissioner's approach, in which

> The purposes for which the card can be used must be settled at the beginning of the project's development; all parties to the smart card project should be identified at the beginning of the project; card holders must be advised before there are any changes to the smart card system (such as the introduction of new features) that affect the collection and use of personal information; their consent – real, informed consent[93] – must be obtained to participate in the new arrangements.

A brief analysis of the Bill (specifically the Access Card) in terms of these guidelines indicates that the ability to prevent function creep will become increasingly difficult to prevent, or to 'retrofit'.

> The purposes for which the card can be used must be settled at the beginning of the project's development.

As discussed, the purposes of the Bill in relation to both the Access Card and Register are established in provisions that are open-ended and clearly will permit additional purposes to be considered (including commercial purposes).

> All parties to the smart card project should be identified at the beginning of the project.

The parties authorised[94] to participate in the use of the Access Card have not been clearly identified. The Federal Privacy Commissioner's guideline recommends *all parties should be identified.* For the Access Card this would include all government agencies; all commercial entities; and all parties involved in manufacturing/producing the smart card and the database.

> Card holders must be advised before there are any changes to the smart card system (such as the introduction of new features) that affect the collection and use of personal information.

transparency of the project is required, that would require all parties to be defined; and limits on collection and use'; Gerrit Hornung's article: *Biometric Identity cards*, at 50, general principles of data protection law require the purpose of the data has to be specified before it is collected and the subsequent use is restricted to those purposes; unless the consent of the data subject or the law provide for this use.

92 Federal Privacy Commissioner, *Smart cards: Implications for privacy*, Information Paper Number 4, December 1995, at 3.

93 The Canadian approach is to treat consent to each of these aspects – 'collection', 'use' and disclosure' as distinct and separate.

94 The Bill, s 72.

The Bill does not address the possibility of how cardholders might be informed of any proposed changes to the Access Card.

> Their consent – real, informed consent – must be obtained to participate in the new arrangements.

The *KPMG Business Case* discussed 'consent' in terms of the Australian public not being required to obtain the Access Card; that it would not be mandatory to apply for the card. However, the reality is that most Australians, who are eligible to entitlements under existing Medicare legislation and social security legislation, will seek continued entitlement under the Bill which requires registration prior to obtaining an Access Card. In turn, an Access Card is necessary in order to obtain a benefit. There is no real opportunity to negotiate on aspects of registration.

Whether or not there is 'consent – real, informed consent' to the original scheme is doubtful. In terms, therefore of 'consent' to any 'new arrangements', it is unlikely that the consultation process to deliver 'real, informed consent' will improve to ensure such a high order consent.

From this analysis there is a high probability that the Access Card and Register will 'evolve so that it will be used for purposes for which [it] was not designed, that never could have been envisaged at the time of [the] system['s] creation'.[95]

The only means to protect against 'function creep' is to pass legislation that cannot be amended without a majority approval of the electorate. The inclusion of a 'prohibited use and disclosure' clause as recommended by the Taskforce, may also offer protection. With respect to the Bill, this would require an express prohibition on expanding the personal information that can be collected, the use of that information, and access to that information. The Bill as currently drafted does not provide this protection.

4.2 Quasi-identity card

This section considers the issue of whether or not the Access Card is in fact an identity card.

[95] *Entitlement cards and identity fraud, Id* Card Response, Stand, January 2003<http://www.stand.org.uk/IdCardResponse.html> at 19.

What is an 'identity card'?

The features of the Access Card that most strongly suggest an identity card include the single universal identifier, for example the unique number that will be assigned to every individual who seeks to claim entitlement under the Bill coupled with the photograph on the Access Card.

How the Bill treats the Access Card in terms of being an identifier

The objects of the Act expressly state, 'that Access Cards are not to be used as, and do not become, national identity cards.'[96] The Bill provides that '[y]ou are not required to carry your Access Card at all times',[97, 98] and the offence provisions make it an offence to require production of an Access Card for identification.[99] However, the Bill also provides that a card-owner may use their Access Card for any lawful purpose.[100] The Explanatory Memorandum acknowledges that 'the Access Card is not a national identity card and is not intended to be used as a national identity card...However; if individuals choose to use the card for identity purposes they may do so.'[101]

Despite the legislative declarations that the Access Card is not intended to become a national identity card, there are three aspects that will almost certainly mean the Access Card will become used as such. The three aspects are: the strengthened proof of identity; the inclusion of the photograph on the surface of the Access Card; and the requirement to register and to obtain an Access Card in order to obtain benefits.

1.'Strengthened proof of identity'

The concept of 'strengthened proof of identity'[102] was initially discussed in considerable detail in the *KPMG Business Case* that envisaged consumers would provide substantial documentation, that they register

[96] The Bill, s 6(2).

[97] The Bill, s 42.

[98] The House of Representatives moved that Clause 42 of the Bill be amended to provide that a person is not required to carry their card 'at any time', not just 'at all times'.

[99] The Bill, s 45.

[100] The Bill, s40.

[101] Explanatory Memorandum, at 14.

[102] This was acknowledged by the *KPMG, Business Case* at 30, also under part 7, 'proof of identity', in which parallel development of a national identity policy with the Attorney General's Department is discussed.

and have their photo taken and that these photos would be matched with their scanned documentation. The Bill has implemented the 'strengthened proof of identity' throughout the provisions dealing with registration[103] and obtaining an Access Card[104] that require the production of information or documents 'needed for the Secretary to be satisfied of your identity'. Both provisions enable the Secretary to request additional documentation 'for the Secretary to be satisfied of your identity'.[105] The Minister is required[106] to prepare 'identity guidelines' that the Secretary must take into account when making specified decisions relating to identity.

However, not all Australian citizens will be able to meet the proof of identity standards, for example the homeless.[107] The Bill has attempted to provide for this by creating a system of marking on the Register and on the microchip of the Access Card whether an applicant's proof of identification is determined to be 'full' or 'interim'.[108] This raises the concern that the dual status will result in a tiered citizenry for cardholders of bearing annotated Access Cards.

2. The photograph

The Bill provides for the storage and display of an applicant's photograph, subject to certain exemptions.[109] The Register will contain the photograph of the registrant that appears on the surface of the Access Card (if one is taken), and 'a numerical template of you derived from that

[103] The Bill, s 13.

[104] The Bill, s 23.

[105] The Bill, ss 13(4), 23(4).

[106] The Bill, s 66.

[107] *KPMG, Business Case* at 30.

[108] The Bill, ss 17(1) Item 8, 34(1) Item 8.

[109] The Bill, s 65(5) allows for certain exemptions from requirements including the requirement to have a photograph taken. Exemptions are not legislative instruments: see s 65(6). The Explanatory Memorandum provides at 58 that 'the general rule in the Bill is that individuals wanting to obtain an Access Card will need to have their photograph taken'. The Explanatory Memorandum acknowledge that it may not be possible for all requirements necessary for the Access Card will be able to be met, for example, attending an interview, having a photograph taken, or providing a signature. The Bill refers to the exemption concerning the photograph with reference to the issuance of the Access Card at s 24(1)(c). It is not entirely clear that the exemption will also apply to the Register. The Bill requires at s 17(1) Item 9, that 'if you own an Access Card... if your photograph is on the surface of your Access Card – that photograph and a numerical template of you derived from that photograph.'

photograph.'[110] The surface of the Access Card will contain the cardholder's photograph.[111] The Commonwealth's area of the microchip in the Access Card will also include the cardholder's photograph as it appears on the surface of the Access Card.[112]

The reference in the Bill to the 'numerical template' is the implementation of the KPMG recommendation of the use of a 'facial biometric template in order to identity duplicate registrants prior to issuing a card.'[113]

The inclusion of the photograph on the face of the Access Card, as well as on the microchip, was considered by the *KPMG Business Case* to be an advantage to increase the potential of the card to be relied upon by non-Department of Human Service officers, including commercial organisations, to use the card as an identifier.[114] For the purposes of the Department of Human Services who have access to the database, and presumably card readers that allow access to the microchip that also contains a photograph of the cardholder, the photograph on the face of the card is unnecessary.

However, it is the inclusion of the photograph on the Register that has the most significant privacy implications because it provides greater potential for the Australian Government's ability to identify and monitor an individual's activities beyond what is necessary for the provision of health and social service entitlements. The Australian Law Reform Commission in its *Review of Privacy, Issues Paper* outlined[115] a number of privacy concerns relating to the use of biometric technologies that allow 'behavioural or physiological attributes of people to be used for identification and authentication'.[116]

For example, with respect to the photograph stored on the Register recordings of individuals taken from public video surveillance can be used to match the identity of registrants. This can occur without the individual's knowledge or consent. Also, there is the potential to deduce

[110] The Bill, s 17(1) Item 9(f).

[111] The Bill, s 30 Item 4.

[112] The Bill, s 34(1) Item 5.

[113] *KPMG, Business Case* at 17.

[114] Ibid.

[115] Australian Law Reform Commission, *Review of Privacy, Issues Paper*, 2006, at 525 – 526.

[116] Australian Law Reform Commission, *Review of Privacy, Issues Paper*, 2006, at 523.

from the photograph sensitive information[117] about an individual (for example, health or religious information). The exemptions from providing the photo given under the Bill[118] do not provide any indications as to the particular grounds for the exemptions, and the Explanatory Memorandum[119] refer to only general grounds for how the administrative power to exempt might be exercised.

A *Biometrics Institute Privacy Code*[120] was recently approved by the Federal Privacy Commissioner. The Code containsthree new information privacy principles that relate to: biometric information to be de-identified; enrolment in biometric systems to be voluntary; and individuals to be informed of the purposes for which a biometric system is deployed.[121] The new information privacy principles might be better contained in the *Privacy Act 1988*, where it would have the force of law, and one would have access to the remedies under that Act.

3. Requirement to register for the card

A key element of identity cards is that they are a 'universal identifier'. Universality implies necessarily that there is a mandatory element in being so identified. The Bill provides registration of the card will be required to obtain the benefits and facilities of the participating agencies which will make the card almost universally required by Australian citizens.

Is the Access Card an identity card?

Professor Graham Greenleaf in his article, '*Quacking like a duck: The national ID card proposal (2006) compared with the Australia Card (1986 – 87)*' undertook a comprehensive comparison of key features of the Access Card with the Australia Card. The comparison compared the following five criteria: A universal, compulsory ID card (compulsion and coverage);[122] card content;[123] the national registration database and access

[117] Australian Law Reform Commission, *Review of Privacy, Issues Paper*, 2006, at 525.

[118] The Bill, section 65.

[119] Explanatory Memorandum, at 58.

[120] I Australian Law Reform Commission, *Review of Privacy, Issues Paper*, 2006, at 526 referring to 'K. Curtis (Privacy Commissioner), 'Privacy Commissioner Approves Biometrics Institute Privacy Code' (Press Release, 27 July 2006).

[121] Australian Law Reform Commission, *Review of Privacy, Issues Paper*, 2006, at 526.

[122] Greenleaf G, 'Quacking like a duck: The national ID Card proposal (2006) compared with the Australia Card (1986 – 87), viewed on the *Cyberspace Law & Policy Centre*

to it;[124] uses of the card[125] and ID number by various sectors; and card-holder's rights and uses.[126]

Professor Greenleaf concluded that 'it is clear that almost all the features present in the Australia Card system are present in the 2006 proposal. In fact, the resemblances are often striking.' The key differences between the two cards were with respect to the smart card technologies that are available in 2006, which were acknowledged to be a greater threat to privacy than the technologies available in 1986.

Implications of an identity card for human rights

Whether or not it is acknowledged that the Access Card is indeed an identity card, a number of human rights issue flow from the fact that a government is readily able to identify its citizens and record their activities.

The right to privacy and the right to information privacy provided for in Article 17 of the *International Covenant on Civil and Political Rights* underpin a number of other human rights that will be compromised without the former right. For example, other rights that may be negatively impacted with the loss of the right to information privacy include: the right to self-determination; the right to liberty of movement; the right to freedom of thought; the right to hold opinions without interference; the right to freedom of expression; the right to freedom of association.

The Australian Law Reform Commission's *Review of Privacy*, states that:[127]

website< http://www.cyberlawcentre.org>, at Table 1, page 2 deals with a comparison of: Compulsion and coverage: whether the card is compulsory; requirement to carry the card; possible confiscation of the card; registration requirements.

[123] Ibid, see Table 2, page 4 that compares the following elements: identification number; card face data; card storage capacity; data on magnetic strip; data on chip (that is both compulsory to provide and that is optional to provide); data related to security.

[124] Ibid, see Table 3, page 6 – the central computer system, card readers and networking, in which the following aspects of both cards are compared: central computer system and content; linked computer systems/access to Register.

[125] Ibid, see Table 4, page 8 – Uses of the Card and ID number by various sectors.

[126] Ibid, see Table 5, page 9 – Card-holder's rights and uses.

[127] Australian Law Reform Commission, *Review of Privacy, Issues Paper*, 2006, at page 556.

the introduction of a unique multi-purpose identifier changes fundamentally the relationship between the individual and the government.[128] In liberal democratic societies governments are accountable to their citizens. It is argued that the introduction of a unique multi-purpose identifier symbolically reverses this tradition, making citizens accountable to their governments.[129]

The Australian Law Reform Commission comment[130] that use of such identifiers, 'increases the ability of the state to monitor the activities of its citizens... [and] [t]he ability of a government to compile dossiers of personal information about an individual could have a 'chilling effect' on the activities of the government's citizen who no longer has a private sphere'[131]

It is difficult to quantify the importance of 'anonymity' and the role it plays in a democratic society. Conversely, the Australian Government has been able to readily (although not necessary accurately) put a figure on the efficiencies to be gained from implementing the Access Card in terms of minimising entitlement fraud. Efficiencies are always there to be gained or worked towards as a government goal; however, once anonymity is lost, the associated rights this concept is allied with such as the right to vote, the right to free speech, the right to freely associate, become increasingly difficult to regain.

If the Access Card has all the features of an identity card, then the requisite debate on an identity card is needed, and the establishing legislation must recognise the Access Card as such.

4.3 Identity fraud

One of the objects of the Bill[132] is to reduce fraud on the Commonwealth in relation to the provision of Commonwealth benefits; the inference (in the absence of further details from the Explanatory Memorandum) can be

[128] Ibid, at page 556 quoting from Parliament of Australia – Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986) [3.7].

[129] Ibid, at 556 quoting G de Q Walker, 'Information as Power: Constitutional Implications of the Identity Numbering and ID Card Proposal' (1986) 16 *Queensland Law Society Journal* 153, 163.

[130] Ibid, at 557.

[131] Ibid, quoting G de Q Walker, 'Information as Power: Constitutional Implications of the Identity Numbering and ID Card Proposal' (1986) 16 *Queensland Law Society Journal* 153, 160 -161.

[132] The Bill, s 6(1)(c).

made that this object of the Bill includes 'identity fraud'. An analysis of the effectiveness of this goal is dealt with in this part of the paper, but first, a brief discussion on what is meant by 'identify fraud'.

Identify fraud can be distinguished from 'identity theft' applying the following definition:[133]

> 'Identity fraud' is often used to refer to where a perpetrator uses another person's personal information, on a limited number of occasions; in a single context (for example, to commit credit card fraud) or in a very limited number of contexts; for material gain. In contrast, 'identity theft' is often used to refer to where a perpetrator uses another person's personal information: on numerous occasions; over an extended period of time; in numerous contexts; for either material or non-material gain.

Using this definition, 'identity theft' may not result in any material gain for the perpetrator, and so allows prosecution without the need to prove 'material gain'. Conversely, 'identity fraud' requires proof of material gain.

The Bill does not distinguish between identity fraud and identity theft, nor does it provide any definitions of either. However both types of offences may occur under the Access Card and the Register. For example, identity fraud may occur in circumstances where a recipient of health or social services entitlements receives that entitlement based on false information about who they are. Identity theft may occur under circumstances in which individual (or group) gains illegal access to the database[134] and uses the personal information gained for either 'material or non-material gain'. Given the extent of information that is required to be uploaded onto the Register, including 'passwords for authenticating your identity'[135] although 'encrypted' may increase the occurrence of identity theft. Even without access to 'passwords', the breadth of information stored in a single location will increase the chances of an unauthorised entrant to the Register (for example, a hacker or authorised person acting without authority) to use a registrants identity fraudulently.

[133] Douglas-Stewart J, 'South Australian laws target identity theft' [2004] PLPR 8; (2004) 10 PLPR 167 downloaded from <http://www.austlii.edu.au//cgi-bin/disp.pl/au/journals/PLPR/2004/8.html?query=identity%20fraud#disp19> and viewed on 7 September 2006.

[134] The Commonwealth Criminal Code sets out offences and penalties associated with illegal access to computer databases.

[135] The Bill, section 17 Item 9(e).

The Bill carries out the object of reducing identity fraud on the Commonwealth through the 'strengthened proof of identity' provisions discussed earlier, and also through the creation of offences in Divisions 3 to 6. For example, it is an offence to change information in the Commonwealth's area of the chip in someone else's Access Card where that person is not authorised to do so, or not the owner; [136] it is also an offence for an owner to change information in the Commonwealth part of the chip; [137] or if it is done with the 'intention of dishonestly obtaining an advantage'.[138] Selling an Access Card is also an offence if it is done either by someone else[139] or the owner. [140]

Division 4 creates a series of offences where Access Cards have been unlawfully obtained; [141] dishonestly obtained; [142] or if the Access Card is 'false'; [143] or an unauthorised copy. [144] Division 5 relates to false or misleading statements in relation to the application process for registration or Access Card in which an applicant is under an express responsibility to ensure all statements are not false or misleading. These offences do not require an 'intention' to mislead.

The penalties for the offences include terms of imprisonment for 2, 5 and 10 years, and fines of 120, 500 and 1000 penalty units.

The Bill does not create any offences regarding information on the Register being dealt with in an unauthorised way. However, Division 6 does create offences by Commonwealth officers, including the abuse of public office[145] that require the intention of dishonestly obtaining an advantage or causing detriment to another. The Explanatory Memorandum[146] state that '[a] major purpose of this clause is to prevent such persons using their position or influence to pressure an official

[136] The Bill, s 48.
[137] The Bill, s 52.
[138] The Bill, s 51.
[139] The Bill, s 49.
[140] The Bill, s 53.
[141] The Bill, s 54.
[142] The Bill, s 55.
[143] The Bill, s 56.
[144] The Bill, s 57.
[145] The Bill, s 62.
[146] Explanatory Memorandum, at 56.

responsible for issuing Access Cards to issue a card for improper purposes'. The penalty is 10 years imprisonment and/or 1000 penalty units. However, none of the offence provisions, including this, deal with an authorised officer viewing or scanning information on the Register for purposes that are not authorised. Neither does the Bill require notification or reparation to 'another' where 'detriment' has been caused to that person.

The offence provisions are mainly concerned with protecting Commonwealth funds from fraud (including identity fraud). This is a proper pursuit and one that government if required to take. However, there is no recognition or protection of rights concerning theft of an individual's identity as being the responsibility of the state. The cost here is solely upon the individual to protect (rather than the state), and it would appear that the burden would be upon the individual to pursue reclaiming their identity.

How does the Bill deal with identity fraud?

The Access Card seeks to address the issue of identity fraud by establishing the Register which 'will contain ... a high quality digital photograph capable of biometric analysis.'[147] The ability to biometrically analyse the photograph is seen as 'important to address identity fraud and prevent duplicate registrations.' [148]

The effectiveness of facial recognition software that detects duplicate registrations

IPPs 7 and 8 require that personal information collected must be accurate, relevant, up-to-date, complete, and not misleading; IPP 4 relates to standards of storage and security. The Bill does not address how it would implement this principle. In reality, the Department of Human Services may experience technical difficulties in complying with these information privacy principles. For example, for the Department to ensure the accuracy and security of the digital photographs, it will need to ensure that the Register does not contain duplicate photographs, which are false identity photographs. Computer programs are available to scan through

[147] *KPMG, Business Case* at 39.

[148] *KPMG, Business Case* at 39.

the Register and identify possible duplicates; however, research[149] conducted on such programs indicates that as the Register size increases, the performance of the technology decreases by a significant percentage. The result is that the program may either falsely detect duplicate photographs, or fail to detect where the same person has been placed two (or more times) on the Register. In terms of the Access Card, it may mean that the Register may still allow false Access Cards to be issued by the Department of Human Services; or that a genuine Access Cardholder is incorrectly alerted to be a false cardholder.

Software dealing with biometric analysis is being researched and developed, and might advance beyond the technology currently available in 2007. Also, the choice of biometric considered the most reliable to be analysed is under consideration by many governments. The prospect of iris scans[150] was included in the *KPMG Business Case*, but paragraphs[151] referring to it have been deleted from the published Business Case making them unavailable for comment. Other biometrics such a voice recognition technology are also under consideration by Australian Government departments.[152]

The Access Card project is vulnerable to identity theft from a number of sources, for example, by outsourced partners involved in the production of the Access Card; through 'hacking' into the Register; from access by Australian government employees (within the DHS, or from other agencies).

Vulnerability of the Register to identity theft

What recognition of the vulnerability of the Register does the Access Card initiative provide? How would it deal with that risk?

The *KPMG Business Case* gives this vulnerability scant recognition. The only reference to this possibility is through a 'Summary of risks'

[149] *Face Recognition Vendor Test 2002, Overview and Summary*, March 2003, P. Jonathon Phillips, Patrick Grother, Ross J Micheals, Duane M Blackburn, Elham Tabassi, Mike Bone, National Institute of Standards and Technology, at 2, 3.

[150] The iris itself is a highly reliable biometric because of its stability, immutability over time, its complexity and the degree of variation in irises between individuals', Justice, *Information Resources on Identity Cards*, December 2004, at 5.

[151] *KPMG, Business Case*, at 20, paragraph 3.7.3, and some sections deleted for 'Cabinet in confidence reasons'.

[152] Ibid, at 21.

regarding the progression of the Access Card project.[153] One of the risks identified, is that of 'security or privacy breach'. This is classified as having a 'moderate' consequence, but a 'rare' likelihood of occurring. The *KPMG Business Case* does not address the risks beyond this general reference, and the Bill provides no recognition of this risk as evidenced through the failure to include an offence provision dealing with potential unauthorised access to the Register.

The risk of identity theft occurring through the Register has been most notably recognised by interest groups responding to the proposed introduction of the Access Card. Electronic Frontiers Australia comments[154] upon the proposal to 'scan in key identity documents such as birth certificates which contain information often used by banks etc as a 'secret' answer' and considers this as making a 'mockery of the (considerably more security and privacy protective) Document Verification Services ('DVS') developed by the Attorney-General's Department.'

The Australian Privacy Foundation[155] expressed more detailed concerns regarding the Register itself, in its statement:

> this centralized database of personal information would likely make identity fraud and theft worse. This is because of a centralised system's vulnerability to hacking, manipulation and corruption. ...the Deputy Commissioner of Taxation [in May 2006, speaking to the AusCert security conference] warned that the 'Access Card' proposal, if implemented, would lead to a rise in identity theft. The proposed national population database, the SCRS, [the Register] would not be any more secure, free from corruption or immune from simple clerical errors than any other database...

In fact, a centralised database has the potential to become a target for identity theft if its contents represent 'strengthened proof of identity'.

[153] Ibid at page 79 and table at page 88.

[154] Electronic Frontiers Australia, *Submission in response to the Taskforce's Discussion Paper*, July 2006, page 12.

[155] Australian Privacy Foundation, *The 'Access Card Proposal: Australian Privacy Foundation's submission in response to Taskforce Discussion Paper No. 1*, 31 July 2006, Sydney, at page 11.

Vulnerability of the smart card to identity theft

Similarly, there are acknowledged weaknesses in the smart card technology that will be used to implement the actual Access Card, as identified[156] in the Australian Government *Smartcard Framework, Smartcard Handbook*. The major security vulnerabilities are considered to include: direct probing, for example by scanning an electron microscope over the smart card to reveal its memory contents; 'side channel' attacks, which have been the subject of much academic and private sector research; crypto analysis; and quantum computing.

Will it be possible to deal with internal fraud and errors?

Recent news reports have drawn public attention to employee breaches of privacy concerning databases that are maintained by the Australian Government. In late August 2006, '19 staff were sacked and 92 resigned after 790 cases of inappropriate accesses by Centrelink staff to client records.[157] Soon after the Centrelink breaches of privacy, the Australian Taxation Office was reported to have taken action against 27 Australian Taxation Officer employees for breaches of privacy. [158] In this case, it was alleged that a number of the 'inappropriate access to taxpayer files' related to events that had occurred during the last financial year.

The report highlights the need for protections offered by information privacy principles that relate to storage and security of information kept by governments.

Part 5 – Conclusion and recommendations

The introduction of the Bill within the existing Australian privacy regime has serious privacy implications. The privacy implications relate to information that appears on the Access Card; within the microchip on the Access Card; and most importantly, regarding the enormous amount of information (both personal and sensitive) that is stored upon the Register. Clear lines of accountability must be established regarding all three aspects of the Bill.

[156] *Smartcard Handbook*, at B21, 8.2: Potential security vulnerabilities.

[157] 'Centrelink breach worries Smartcard boss', August 23, 2006, <http://www.theage.com.au/news/National/Centrelink-breach-worries-Smartcard-boss/...> viewed on 31 August 2006.

[158] 'ATO sacks staff over privacy breaches', August 29, 2006, <http://www.news.com.au/story/o,10117,20288523-1702,00.html?from=public_rss> viewed 31 August 2006.

Already, the Bill creates breaches of information privacy principles provided for under the *Privacy Act 1988*. It is likely that these breaches will lead to significant function creep of both the Access Card and the Register to the extent that it will become used for purposes beyond those relating to the entitlement to health and social services. Further, the Access Card may offer no better protection against false health and social security claims to entitlement, whilst the Register has the potential for increasing identity theft.

The following recommendations would provide some limited form of privacy protections:

That the Health & Social Services Smart Card Management Authority be reinstated by legislation to provide independent and expert oversight of the Access Card and the Register.

That the role of the Federal Privacy Commissioner be given statutory recognition to ensure consistency between the *Privacy Act 1988* and the *Human Services (Enhanced Service Delivery) Bill 2007*, and to provide consultation and advice on all aspects that breach privacy principles.

That legislation expressly specifies the limits of access to the information of the Access Card and expressly protects the purposes for which the personal information can be used, as well as the prohibited uses.

That the Register be given express legislative protections including prohibition on data-matching; limitations upon the scanning of proof of identity documents; limitations on the use and disclosure of biometrics including the photograph; and that the offences include unauthorised access to, use of, and disclosure of information on the Register.

That the Bill include a statutory duty regarding the security, integrity and accuracy of information kept on its databases, and that appropriate compliance and enforcement procedures be developed and implemented.

The ability of a government to accumulate personal information will increase with the development of invasive technologies that are able to map and determine identifying characteristics of an individual. In 2008, the Register will be able to record and store information in terms of name, address and limited biometrics such as a photograph. In 2018, the technologies capable of recording details of information and biometrics will relate to, at the very least, the genetics of an individual. Now is the

time to consider the capabilities of the Register and the Access Card, and put in place legislative protections to safeguard the right to information privacy and the human rights that are so closely aligned to it.