The Health and Social Services Access Card: What will it mean for Australians?

Financial Literacy, Banking and Identity Conference
25th and 26th October 2006
RMIT University, Melbourne

Professor Margaret Jackson and Julian Ligertwood, School of Accounting and Law, RMIT, and CRC for Smart Internet Technology

Abstract

This paper provides a history of identity documents in Australia and of the events leading up to the recent government proposal for a health and social services smartcard known as the Access card. It examines the reasons behind the government's decision to proceed with the Access card as well as the features that it will contain. Various criticisms in relation to the card are discussed including the proposed purpose of the card, the administrative scheme, and the adequacy of privacy protection. Some conclusions are drawn about whether, despite the government's claims, the card represents a de facto national identity card.

1 Introduction

The Australian Government announced in April 2006 that it was introducing a health and social services smartcard to be known as an ‘Access card’. This Access card will be available from 2008 to any Australian who registers and who is entitled to claim health or social service benefits such as Medicare, unemployment benefits and an age pension. It will replace 17 existing cards. The Government has announced that the Access card ‘is not a national identity card. It will not be mandatory to apply for one and there is no requirement to carry or produce the card’ (Ruddock 2006), however, all adult Australians will be eligible to register for the card and are expected to do so as it will be the only way to obtain Medicare refunds and other government services.

This paper examines the lead up to the announcement of the Access card and the reasons given by the Government for its decision to proceed with the health services card rather than a national identity card. It also examines the limited amount of information the Government has released to date about the Access card to assess what concerns about it have been expressed. Finally, it discusses whether the Access card is likely to become a de facto national identity card despite the Government's statements.
2 The Medicare Card and Discussions about its Replacement

2.1 The Medicare Card

Australians are entitled to obtain subsidised health and hospital care. The government health care insurance scheme was first known as Medibank when introduced in 1974, and then as Medicare after the scheme was amended in 1983 (Scotton 2000). As a part of the scheme, all Australian adults are issued with a card which contains a unique number, a name and an expiry date. It does not contain a signature. The card is issued to all adult Australians although children over the age of 15 years may apply for their own card (Medicare 2006). Also, one card may be issued to a family group rather than to individuals of the family, so that the names of the parents and dependent children are shown on the card. According to Medicare, as at June 2005, there were 20.5 million people enrolled in Medicare and 11.4 million ‘active’ cards (Medicare 2006).

There is no requirement to carry the Medicare card. It must be produced, however, when seeking reimbursement of or payment for health and hospital bills, when seeking medicines covered by the Pharmaceutical Benefits Scheme (PBS), and to place children on the Australian Childhood Immunisation Register.

There are two separate databases linked to the Medicare card, one dealing with Medicare claims and the other with PBS claims. The content of each database is not known definitely but the Office of the Federal Privacy Commissioner understands that the following information is held:

On the Medicare database:
- the name and address of the individual
- the name of the provider (for example, the doctor or hospital) and the provider’s Medicare Australia number and ABN number
- the item number, that being the number that identifies the type of service provided (this can also include a general description of the service, such as “Level B surgery consultation”)
- the cost of the service
- the date the service was provided and
- whether the service has been paid for (OFPC 2006, p 16).

The PBS claims information held by Medicare Australia includes:
- the name and address of the individual
- Medicare number
- information about the prescription, including the date it was written and issued, the item number, the type of script, quantity, dosage and any repeats
- the prescribing doctor
- the pharmacy supplier and
- the patient contribution to the cost of the script (OFPC 2006, p 16).

According to the Privacy Commissioner:

Medicare claims information is not stored by the individual’s name or Medicare card number, but by a Medicare PIN (Personal Information Number) generated internally by Medicare Australia… [T]he PIN is a unique number for each individual, and is not generated from the individual’s Medicare card number, address or date of birth (OFPC 2006, p 16).

These databases are required to be kept separate but privacy guidelines state the limited ways in which these databases can be accessed by government departments (OFPC 2006).
2.2 Medicare Smartcard

A Medicare smartcard was launched in July 2004 as part of the Government’s ‘commitment to using better information to deliver better quality health services’ (Abbott 2004). The press release issued by the Minister for Health and Aging justified the introduction of the smartcard as follows:

About 3600 hospital deaths per year are attributed, in part, to inadequate health information. At least some of those deaths could be avoided if treating health professionals had better access to their patients’ records (Abbott 2004).

The smartcard has the same physical appearance as the Medicare card and holds the same information with the optional choice of including a digital photo which is stored on the chip and is not visible on the card. It can also store optional information about allergies and adverse drug reactions. It can be used as a family card or individual card in the same way as the standard Medicare card.

The smartcard was trialled in Tasmania and was intended to be made available to the rest of Australia in line with the HealthConnect initiative which involves the national storing and accessing of electronic health records (Medicare 2006). Participation in the smartcard trial was voluntary but only about 3000 people or 1 per cent of the population volunteered. On 25 May 2006, the Government announced it would not proceed with the trial, giving the introduction of the Health Services Access card discussed below as the main reason for its cessation (Deane 2006), even though the stated purposes of the Medicare smartcard would not be met by the Access card.

3 The Australian Government proposals for the Access Card

3.1 Background to Identity Cards in Australia

The idea of a national identity card is not new to Australia as it has a history of registration, personal identification and data collection within both the public and private sectors. During WWII, Australians were registered under the National Security Act 1939 (Cth) and National Registration Act 1939 (Cth) and were given a basic identity card under the 1947 National Security (Manpower) Regulations. The imposition of rations was an incentive for registration and production of the card (Caslon 2005).

It was not for another thirty years, however, before three government reports published in 1975 suggested that government efficiency could be improved and fraud better detected through the introduction of an identity card system (Jordan 2006). The then Fraser Government took no action about these recommendations at that time. In 1986, the Hawke Government tried to introduce a national identity card, the Australia Card, but there was substantial public opposition to it and, by 1987, 90 per cent of Australians were opposed to the card (Davies 2004). However, the accompanying Privacy Bill 1988 (Cth), which contained Information Privacy Principles about how personal information was to be collected by federal government agencies, was enacted and enhancements to the Tax File Number (TFN) scheme administered by the Australian Taxation Office (ATO) were enacted with the objective of increasing the Government’s capacity to link the identification of specific taxpayers with specific taxable income (Clarke 1987).

The next attempt to introduce a national identity card in Australia apparently began as a result of the London bombings on 7 July 2005. On 14 July 2005, Queensland Premier Peter Beattie commented on the issue on ABC radio arguing that such a card would be in the interests of national security. When asked about Beattie’s comments, Prime Minister Howard did not support them but his own comments were vague and he was reported in the press as not ruling it out altogether in the Government’s review of security arrangements (Humphries and Todd 2005). Howard then became more supportive of the idea of an identity card and the Attorney-General subsequently stated that the Government would be examining the possibility of an identity card (Howden, Crawshaw, and Tasker 2005; Australian Privacy Foundation 2005). However, many government ministers were strongly opposed to the idea as the Attorney General himself had been in October 2003 (Baker 2006).

In January 2006, Attorney-General Philip Ruddock announced he was establishing a formal enquiry into whether Australia needed an identity card and how much it would cost to implement it (Priest 2006). He provided no specific information about the purpose of such a card so that it was not clear if the primary focus would be on security, identity fraud, anti-money-laundering or effective government services. However, in an abrupt turnaround, the Prime Minister and the Attorney-General announced in April that the Government would not be introducing a national identity card but would instead introduce a health and welfare services smartcard (Gratten 2006; Crawshaw 2006).
3.2 Current Proposal – the Access Card

The new government card was first raised as a possibility by the Human Services Minister, Joe Hockey, in April 2005 and at that stage, the main objectives of the ‘Human Services Smartcard’ were to reduce welfare fraud and to enable 3.6 million social security recipients to access benefits (Bajkowski 2005; Schubert 2005). By July 2005, it had become the ‘Government Services Card’ (Schubert 2005) and was to contain a photo and replace 26 government services cards and concession cards. Its cost was estimated to be $500 million. In January 2006, Hockey stated that the card would be a compulsory identity card for all welfare recipients and would contain biometric data (Riley 2006). In March 2006, it was to be used so patients could get medical bill reimbursements from EFTPOS machines in surgeries, to stop welfare fraud and to assist with disaster relief but it would still only be compulsory for the provision of government services (Bajkowski 2006; Sutherland 2006).

The proposal for a human services smartcard was discussed at a Cabinet meeting on 26 April 2006. A year after it had first been discussed by Minister Hockey, its objectives continued to evolve. Now the major purpose of the smartcard, to be phased in from 2008, is to prevent welfare fraud. The card will replace 17 existing benefits cards. The cost of setting up the smartcard is about $1 billion over four years (Grattan 2006).

The Government further states that it will not be compulsory to have or carry the card, unless the individual requires health or government services (Ruddock 2006). However, as all adults and children over the age of 15 are required to have the card, if they wish to be reimbursed for health expenses, the new smartcard will be, in effect, compulsory for the majority of Australians. KPMG, the author of the Government’s business case report for the Access card, entitled ‘The Health and Social Services Smartcard Initiative Volume 1: Business Case Public Extract’, estimates that at least 16 million Australians will be issued with an Access card, almost three quarters of the population (KPMG 2006).

3.3 The Form of the Access Card

The Access card will be a plastic card containing a microchip (Access Card Taskforce 2006). On the front of the card will be the cardholder’s name and photograph, and on the back will be the cardholder’s reformatted Medicare number and digital signature. The chip will contain data such as a photograph, data of birth, address and names of dependants, in addition to optional information relevant to a medical emergency.

Registration for the card will be facilitated by the Secure Customer Registration Service (SCRS) which, in addition to the information on each card, will contain an individual’s address, date of birth, documentation presented during registration, dependant information, concession status, and a flag for each of the agencies with whom the customer has an existing relationship. The Government has stated that the SCRS will not contain any agency specific data, nor will it provide agencies with access to other agencies’ data (Access Card Taskforce 2006). However, all Department of Human Services agencies and the Department of Veteran’s Affairs will have access to the database (KPMG 2006). It is understood that individuals will be able to update the information about themselves stored on the Access card database but how this will work is not clear (KPMG 2006). The KPMG Report also states that individuals can update and change personal information online but also states that the Access card will be updated at the same time. No detail of how this would happen is provided.

The Minister for Human Services established the Access Card Consumer and Privacy Taskforce (the Taskforce), chaired by Professor Alan Fells, to advise the Government on issues such as consumer privacy, appropriate registration procedures, technology and legislation (Access Card Taskforce 2006). In June 2006, the Taskforce released a discussion paper, titled ‘The Australian Government Health and Social Services Smartcard’, raising what it considered to be the relevant issues. The Taskforce invited submissions and a broad range of individuals, organisations, privacy and industry groups have responded, voicing concerns about the Access card, particularly in relation to its similarities to a national identity card scheme.
4 Issues and Criticisms

The Government says that consumers will benefit from the introduction of the card because it will improve the delivery of government services and will reduce fraud (Access Card Taskforce 2006). KPMG (2006) estimated that, over ten years, the Access card would help save up to three billion dollars lost as a result of fraud and administrative error. However, these figures have been disputed. Electronic Frontiers Australia (EFA), for instance, maintains that there is no basis for such a figure, particularly as it includes in its definition of health and welfare fraud those cases where people have inadvertently or unintentionally failed to notify the Government agency of relevant changes in their circumstances (EFA 2006). In its view, this sort of fraud could not be prevented by an identity card. Similarly the Health Issues Centre (HIC) in its submission to the Taskforce criticized the KPMG figures. HIC points out that there is no detailed discussion of fraud in the KPMG report and therefore it is uncertain whether fraud is actually identity fraud as opposed to, say, failing to divulge employment. HIC also believed that the costs of administering the Access card will be far greater than predicted by the Government and KPMG (HIC 2006).

Interestingly the Government will not be releasing those sections of the KPMG Report relating to the predicted savings that can be made from the introduction of a national smart card to combat welfare fraud. Federal Minister of Health and Aging, Tony Abbott, has even cast doubt over whether the savings being predicted will be realised:

It's not normally Government practice to release these kinds of documents. The $3 billion worth of saving is inevitably an estimate because we're talking about $3 billion worth of savings over about a decade, so there's no exact science here (ABC News Online 2006).

A political movement against the Access card scheme has started to gain momentum. A group of Liberal Party members in Victoria are lobbying against the proposal, as is the Civil Liberties Australia lobby group, the Australian Chamber of Commerce and Industry, and the Public Interest Advocacy Centre. They argue that the alleged benefits of the Access card do not justify the expense nor the threat to privacy, and that the Government appears unwilling to publicly debate these issues (Dearne 2006).

Probably the main criticism of the Access card is that there is very little data available about how it will operate. However, there are many other criticisms contained in the submissions to the Taskforce which can be located at http://www.humanservices.gov.au/access/discussion_papers/index.htm. The issues raised in submissions include those discussed below.

Inadequate privacy protection

The Taskforce discussion paper raises three major privacy questions in relation to the Access card. First, is the current proposal to include a unique identifier on the card valid with respect to current data protection laws? Second, is the existing privacy legislation adequate in light of the Access card proposal? (The Victorian Privacy Commissioner does not believe so. He predicts that the current Australian Law Reform Commission inquiry into the Privacy Act may well insist on a more stringent privacy regime (Victorian Privacy Commissioner 2006)). The third question is, which body should be responsible for the oversight of the access card system and should it be independent of government so that citizens can be confident that their privacy rights are being protected (Access Card Taskforce 2006)? At present, oversight of the Access card rests with Minister Hockey's Department and not, as recommended in the KPMG Report, with an independent body (KPMG 2006)

The Government claims that having only the name, photograph, card number and digital signature visible on the card, and the storage of personal verification data on the chip in a database will ensure security and privacy (Access Card Taskforce 2006). However, many privacy advocates argue that a large centralised database increases the risks to privacy and security (Victorian Privacy Commissioner 2006, EFA 2006). They also question the security measure of having visible personal data on both sides of the card. And yet the question must be asked, what value would the card be without this visible data? The Taskforce is concerned that the collection of photographs of the vast majority of Australians on the SCRS may also be a risk to privacy. In particular, a database of digital photos would enable data matching of these with records generated and stored by other electronic means such as CCTV unless physical security of the system is ensured (Access Card Taskforce 2006).

Registration and issuing procedures
Several questions arise in relation to registration and card issuing procedures, most notably how the Government will deal with people with disabilities or people with religious and cultural objections to the card. Also, how is identity to be established if primary identifying documents are unavailable? How will the system deal with people (generally the disadvantaged) who regularly lose their card (Access Card Taskforce 2006)? The Victorian Privacy Commissioner raises the issue of whether the card is to be withdrawn or suspended by the Government, for example, if a person is imprisoned or incapacitated, and what the implications of this will be (Victorian Privacy Commissioner 2006).

**Authorisation, Accountability and Function Creep**

The Taskforce points out that it is important to determine the extent to which legislation should be used to establish and govern the Access card system, making clear the permitted and prohibited uses. In particular, it still needs to be determined what aspects of the Access card system should be placed in legislation, what appropriate accountability arrangements should be introduced and whether or not records will be kept of who has accessed the system (Access Card Taskforce 2006). As well, if individuals are able to access and update their own data, such activity causes its own set of security and data accuracy problems. Rights of access must be clearly regulated and subject to independent oversight.

Access to some of the data on the Access card is to be provided to a range of entities and individuals, including medical practices, pharmacies, ambulances, hospitals, allied health workers, but how much of the data stored on the card will be accessible is not known (KPMG 2006). This is a matter of concern to many individuals lodging submissions to the Taskforce, more so, in fact, than the concern that personal information is to be handed over to the Government. The Federal Privacy Commissioner noted in her submission to the Access card Taskforce that:

> Recent international comparative research conducted by Accenture found significant difference in the degrees of comfort individuals had with government departments sharing data depending on what the data was. While there is some comfort around the sharing of information such as name and date of birth, this diminishes considerably when the data being shared is medical records, or information related to social security, social insurance or national tax numbers (Privacy Commissioner 2006, p 53).

There are also many concerns about ‘function creep’. This term refers to the way in which systems introduced for one purpose morph over time to serve quite different purposes. Although the SCRS will be established separately from the databases already held by Department of Human Services units, its existence may encourage the Government to match data from different agencies. The Taskforce urges that such activity would either have to be prohibited or strictly regulated (Access Card Taskforce 2006). The Victorian Privacy Commissioner also believes that a purpose built statute is necessary for the scheme because of the likelihood of function creep over time, as government and business find new uses for the card. He points out that function creep is not a priori bad, but it is necessary to plan for it with open, legitimate and reviewable processes (Victorian Privacy Commissioner 2006).

Other uses of the card proposed by KPMG include disaster relief payments via ATMs and EFTPOS terminals at banks and retail outlets and its use as an identity card by state agencies. This is an early indication that the smartcard will be subject to function creep with the possibility of more and more public and private organisations gaining access to the personal information held on the card. The use by state authorities, in particular, raises the question of whether the Access card will become an identity card by default. As well, it is not clear how the Government will use the Access card as it proceeds with the HealthConnect initiative for electronic health records.

**Unauthorised Access**

A key concern is how the system will ensure that SCRS data is only accessed for authorised purposes. Unauthorised access to confidential government databases appears to occur at regular intervals. In 1990, the New South Wales Independent Commission Against Corruption (ICAC) commenced a two year enquiry into the problem (Jackson 1993).

ICAC found a widespread trade in government confidential information existed at both state and Commonwealth level involving the public and private sectors. Involved in this trade were members of the New South Wales police, New South Wales Road Traffic Authority officers and other state and Commonwealth public officers, insurance companies, banks and other financial institutions, and private enquiry and commercial agents.
At state level, the information released included driver's licence and motor vehicle registration particulars, police records, and the records of electricity suppliers. At the Commonwealth Government level, confidential information from the Department of Social Security, Telecom, Australia Post, the Department of Immigration, the Australian Taxation Office and Medicare, had been released or traded. The information, which concerned private individuals and commercial enterprises, was normally requested from a government official by an insurance company, bank or other financial institution. In most, but not all, cases, the official sold the information for cash. ICAC found that a total of 155 people had engaged in corrupt conduct and a further 101 had 'engaged in conduct which allowed, encouraged or caused the occurrence of corrupt conduct' (ICAC 1992, p 7).

The ultimate purchasers of the information included all the major Australian banks, insurance companies, finance companies, large trading corporations, and at least one firm of solicitors. There was no doubt that those institutions which requested the information were fully aware that access to it by them was not unauthorised.

In 1995, the Commonwealth House of Representatives Standing Committee on Legal and Constitutional Affairs released In Confidence: A Report on the Protection of Confidential Personal and Commercial Information held by the Commonwealth which examined the adequacy of the existing protection for confidential personal and commercial information (third party information) held by the Commonwealth Government and its agencies. An important finding of the Committee was that no privacy ethos existed in Commonwealth agencies. It placed most of the blame for this lack of commitment to privacy on senior managers (In Confidence 1995).

More recently, there have been four reported cases of unauthorised access to personal information by Government officials. A Centrelink investigation has uncovered 858 cases of ‘breaches of privacy/confidentiality or conflicts of interest’ to the records of welfare recipients since 2003 (Centrelink 2006, p 116). Five of the cases have been referred to the Australian Federal Police for possible prosecution. Some 19 staff were sacked, and 92 resigned when faced with accusations of inappropriate breaches of privacy. More than 300 staff faced salary deductions or fines, another 46 were reprimanded, and the remainder were demoted or warned (ZDNet 2006).

In addition to Centrelink, the Australian Taxation Office (ATO) has confirmed that it has recently taken disciplinary action against 27 employees for breaches of privacy (Anderson 2006). Four were sacked. ATO management took action after the staff members were caught accessing taxpayer files without authorisation last financial year. The Tax Commissioner has denied that personal information was released inappropriately.

In Victoria, there have been a number of cases involving unauthorised access to, use of and disclosure of confidential police files. Five officers inappropriately accessed the file of victims' rights campaigner and political candidate, Kay Nesbit, before the 2002 state election (The Age 2004). In June 2005, a woman in country Victoria, known as Jenny, was accidentally sent 490 confidential police files by the Office of Police Integrity after a series of mailroom blunders (Victorian Privacy Commissioner 2006b). In July last year, Victoria Police mistakenly released more than 7000 pages of files to a prison officer turned whistleblower (Victorian Privacy Commissioner 2006c).
Will the Access Card become a Defacto National Identity Card?

5.1 What is a National Identity Card Scheme?

An identity card scheme will obviously seek to identify an individual through the information on the face of or stored on a chip in the card. Identity card schemes may operate for a single purpose, such as to identify those people who are licensed to drive a car, or to provide a means of identifying a particular class of person, say those entitled to specific government entitlements or pensions.

In 1996 around 100 countries had compulsory identity cards (Privacy International 2006) The term “compulsory” may have different meanings and implications in different countries. The compulsory character may apply only after a certain age. Often, a ticket can be given for being found without one’s identification document, or in some cases a person may even be detained until the identity is ascertained. In practice, random controls are rare, except in police states.

A number of countries have non-compulsory identity card schemes. These include Austria, Canada, Finland, France, Iceland, Sweden, Switzerland. A number of countries do not use identity cards to verify identity. These include Denmark, India, Ireland, Japan, New Zealand, Norway, and the United States. (Wikipedia 2006). However, India is currently piloting an ID card system (Indian Express 2006).

There is no national identity card in the United States of America. All attempts to create one have not been realised due to political disagreements over infringement of privacy. Driver’s licenses issued by the various states (along with special cards issued to non-drivers) are often used as proof of identity and a national identification card is often required for boarding airline flights or entering office buildings. Recent federal legislation that tightened requirements for issuance of driver's licenses has been seen by both supporters and critics as bringing the United States much closer to a de facto national identity card system (Wikipedia 2006).

Australians already carry a number of identity cards, such as their driver’s licence. Not all Australians drive, however. Many Australians possess a passport, but only those who wish to travel overseas. Two national government-provided identifying numbers are issued to virtually all adult Australians – a Medicare number and a Tax File Number (TFN). The Medicare number is issued to all adult Australians on a plastic card with their name on it. The number is linked to a database which contains personal information about the individual but the card itself has no signature or photo and it is not required to be carried. The TFN is just that – a number, although it is linked to a database containing extensive personal information and is used for authorised government data matching purposes. National Privacy Principles 2 and 8 in the Privacy Act state that neither of these numbers can be used to identify a person. The most commonly used personal identification used by business in Australia is a driver’s licence, as it contains a photo and address details.

Generally, a national identity card scheme, as opposed to an identity scheme for a specified purpose, involves the collection of personal identifying information to be stored in a computer database created by and managed by the government, and the issuing of a card with personal details on it, normally a photo, a number and signature. All adults must be issued with the card and usually but not always are required to carry it on them at all times.

The United Kingdom (UK) Government recently introduced a national identity card scheme. The Identity Cards Act 2006 was enacted in March 2006. The following information about an individual, generally all people residing in the UK over 16 years of age, will be collected and retained in the Register, includes:

- Full names and other known names
- Date and place of birth (and date of death)
- Gender
- Physical characteristics
- Biometric information (which could include signatures, facial recognition, digital photos, iris scans or fingerprints)
- Every residential address with dates
- Nationality
- National Identity Registration number, identity card number, National insurance number, passport number, driver's licence, work permits, immigration documents as well as other reference numbers allocated
- Validation information – including information provided to support initial registration or a modification to it
- ‘Steps taken’ by the authorities to identify an individual or verify information provided to the Register
- Security information, such as a PIN number, password or code, for the purpose of providing information to the register
- information about occasions on which information recorded about an individual in the Register has been provided to any person.

The Act empowers the Secretary of State to enforce registration (s7). Interestingly, it will not be compulsory to carry a card (s13(3)) and, with the exception for the provision of public services or where a person is given the option of using reasonable alternative methods of establishing their identity (s13), it will be unlawful to require an individual to produce an identity card (s16).

The UK scheme centres around the creation of a national register which will be able to be accessed by over 265 government departments and, if the individual consents, by about 44,000 private sector organisations (London School of Economics 2006). By opening up access to the database to the private sector and to all government departments, the Government is encouraging the use of the Identity card in a way that is inconsistent with the fact that it doesn’t have to be carried or produced on demand.

The UK Government argued that the Identity card will tackle crime that relies on the use of false identities, such as terrorism, drug trafficking, money laundering, fraud through identity theft, illegal employment and immigration. Also, the Identity card will enable people to access current services more easily, provide a watertight proof of identity for use in everyday transactions and travel, and provide a means of providing more efficient services (London School of Economics 2006).

The UK Government has not been able to show clearly, however, how its Identity card and Register will reduce terrorism and other security threats, although this is part of the stated purpose for their introduction. Also, when the London School of Economics (LSE) examined government statistics from 2002 on the cost of identity fraud, it concluded that the card would have no or very minor impact on identity related VAT fraud, money-laundering (as identified by Customs and Excise), health services fraud, immigration fraud, insurance fraud, credit card fraud, and identity theft fraud (London School of Economics 2005). The only category of identity fraud in which an identity card could be used effectively was that of identity related social benefit fraud, estimated to be approximately £35 million per annum (or 1% of total benefit fraud) (London School of Economics 2005). There is also a possible use in stopping temporary workers from outstaying their entry visas.
5.2 A Defacto Identity Card?

The Access card will be issued to all adult Australians. It will contain a photo and signature. It will be linked to a government database. It will not, according to the government, be required to be carried at all times but, then, the UK Identity card will not have to be carried at all times either. The Government has maintained that obtaining the Access card will be voluntary. However, most Australians are eligible for Medicare so in effect almost every Australian will at some stage need to obtain the Access card to be able to access government health reimbursements (Access Card Taskforce 2006).

So will it become a de facto identity card? It has been stressed by the Taskforce in its discussion paper and by privacy groups that it is very important that the Access card does not become a national identity card by stealth (Access Card Taskforce 2006, APF 2006; EPA 2006). Although the Government denies that there is a risk of this happening (Crawshaw 2006), many believe that the current proposal for the Access card already has the features of an identity card (Greenleaf 2006; APF 2006). For example, the Victorian Privacy Commissioner points out that the card’s photograph will inevitably lead to people being required to produce the card for purposes other than those for which the card was issued, thus becoming a de facto identity card (Victorian Privacy Commissioner 2006).

Identity cards per se are not ‘bad’. Australians are used to different forms of identity cards already. The main question arising from any proposal to introduce any form of identity card is whether its negative impact on the human and legal rights of citizens is sufficiently balanced by the benefits arising from the reduction of the problems it is designed to reduce, such as identity fraud or threats to national security. There are, of course, many other questions relating to the feasibility of the technology proposed and the cost of the scheme but these are beyond the scope of this paper.

The multifunctional nature of the proposed Access smartcard causes alarm. The entire adult population does not need a card for the Government to stop welfare fraud; only those receiving welfare payments. The Australian Government has stated that the main purpose of the Access Card is to reduce social security fraud but has not yet provided convincing statistics relating to identity-related social services fraud to demonstrate what the savings might be and how they will be achieved.

There can be little doubt that the 100 points currently required for identification will be amended to allow for the introduction of the Access card as one identifier. The growing use of existing identity cards to prove identity when buying goods, opening banks accounts, etc, means that the only way that the Access card will not become a national identity card is if the Government legislates to both prohibit its use for that purpose and to restrict access to the SCRS for any purpose other than the provision of government health and social security services.
6. Conclusion

The Attorney-General removed the identity card debate altogether from the Federal Government’s agenda, apparently as part of government strategy to proceed with the Access card. However, whilst originally proposed as a way to reduce social security fraud, the Access card appears already to be undergoing function creep and is to be used as a new Medicare card, for the provision of all government services, for disaster relief and so on.

The Government has not yet released full details of the Access card scheme. Most of the information available has come from government briefings to the media, from an overview of the Access card on the website of the Human Services Minister, from the KPMG Report, and now from the Taskforce Report.

There are a number of privacy issues associated with the proposal, particularly around the extent of third party access, the breadth of the data being collected, and the introduction of additional uses for the data which may not be explained to individuals at the time they supply their personal information. Until further details are available, however, it is not possible to discuss them further. It is imperative that when the full extent of the Access card scheme is released, there has been appropriate discussion with the Privacy Commissioner and the opportunity for broad consultation.

No matter what name the card is given, it is imperative that the objectives of the scheme are precisely articulated so that there can be an appropriate evaluation of how the scheme would address those objectives. The need for a national scheme of any type for any purpose will have to be demonstrated compellingly and the barriers to be placed around the data collected so that both authorised and unauthorised access is reduced need to be strong.
References


• Gratten, M, ‘Smartcard to replace 17 others’ The Age, 27 April 2006.


• Health Issues Centre (HIC), Submission to Access Card Consumer and Privacy Taskforce on the proposed Health and Social Services Access Card, 27 July 2006.


• Howden, S, Crawshaw, D, Tasker, B, ‘PM puts ID card firmly back on the agenda’ Sydney Morning Herald, 16 July 2005.


• Jackson, M 2001, Hughes on Data Protection Law in Australia, LawBook Co.


• ‘Numbered Lives’, Indian Express, 20 August 2006


• Office of the Victorian Privacy Commissioner Report 03.06, Mr C’s Case: Report of an Investigation pursuant to Part 6 of the Information Privacy Act 2000 into Victoria Police and Department in relation to security of Personal information in the Law Enforcement Assistance Program (LEAP) and E – Justice Databases, July 2006 http://www.privacy.vic.gov.au/dir100/piweb.nsf/content/5d37ecb57a98bda7ca256c4d0019e8ad?OpenDocument&ExpandSection=1#_Section1, accessed 6 September 2006


