

The Senate

---

Standing Committee on  
Finance and Public Administration

---

Human Services (Enhanced Service  
Delivery) Bill 2007 [Provisions]

March 2007

© Commonwealth of Australia 2007

ISBN 978-0-642-71781-8

Printed by the Senate Printing Unit, Parliament House, Canberra.

# Senate Finance and Public Administration Committee

## Members

Senator Brett Mason, Chair	Queensland, LP
Senator Michael Forshaw, Deputy Chair	New South Wales, ALP
Senator Carol Brown	Tasmania, ALP
Senator Concetta Fierravanti-Wells	New South Wales, LP
Senator Mitch Fifield	Victoria, LP
Senator Claire Moore	Queensland, ALP
Senator Andrew Murray	Western Australia, AD
Senator John Watson	Tasmania, LP

## Substitute Member

Senator Stott Despoja to replace Senator Murray for the Committee's inquiry into the provisions of the Human Services (Enhanced Service Delivery) Bill 2007

## Participating Member involved in the inquiry

Senator Kate Lundy

## Secretariat

Mr Alistair Sands, Secretary  
Mr Terry Brown, Principal Research Officer  
Ms Monika Kruesmann, Principal Research Officer  
Ms Sharon Babyack, Estimates/Research Officer  
Ms Emma Hardman, Executive Assistant  
Ms Judith Wuest, Executive Assistant

PO Box 6100  
Parliament House  
Canberra ACT 2600  
Ph: 02 6277 3540  
Fax: 02 6277 5719  
E-mail: [fpa.sen@aph.gov.au](mailto:fpa.sen@aph.gov.au)  
Internet: [http://www.aph.gov.au/senate\\_fpa](http://www.aph.gov.au/senate_fpa)



# TABLE OF CONTENTS

<b>Membership of Committee</b>	<b>iii</b>
<b>Chapter 1</b>	<b>1</b>
<b>Introduction</b>	
Background	1
Purpose of the bill	1
Conduct of the Inquiry	2
Acknowledgement	3
Note on references	3
<b>Chapter 2</b>	<b>5</b>
<b>Overview of the bill</b>	
Provisions of the bill	5
<b>Chapter 3</b>	<b>11</b>
<b>Key issues</b>	
Introduction	11
Timing issues	12
The Card – surface information	14
The chip inside the card	24
The register	26
Discretions and Delegations	31
Administrative review	37
Access	38
Offences	43
Issues not considered	45
Conclusion	46

<b>ALP SENATORS' ADDITIONAL COMMENTS</b>	<b>49</b>
<b>THE AUSTRALIAN DEMOCRATS ADDITIONAL REMARKS</b>	<b>57</b>
<b>AUSTRALIAN GREENS ADDITIONAL COMMENTS AND RECOMMENDATIONS</b>	<b>85</b>
<b>ADDITIONAL COMMENTS BY SENATOR FIERRAVANTI-WELLS</b>	<b>93</b>
<b>Appendix 1</b>	<b>97</b>
<b>Submissions Received</b>	
<b>Appendix 2</b>	<b>101</b>
<b>Additional Information and Related Evidence</b>	
<b>Related Evidence</b>	<b>101</b>
<b>Appendix 3</b>	<b>103</b>
<b>Public Hearings and Witnesses</b>	

# Chapter 1

## Introduction

### Background

1.1 On 8 February 2007, the Senate referred the provisions of the Human Services (Enhanced Service Delivery) Bill 2007 to the Finance and Public Administration Committee for inquiry and report by 15 March 2007, on the recommendation of the Selection of Bills Committee.

1.2 The Committee was charged with examining, among other things, the bill's provisions relating to the intended scope and purposes of the card; the information to be included in the card register and the card's chip and on the card's surface; and the range of offences aimed at prohibiting persons requiring an access card for identification purposes and prohibiting other improper uses of the card.

### Purpose of the bill

1.3 The purpose of the bill is to facilitate the provision by participating agencies of benefits, services, programs, or facilities to some or all members of the public, through establishing a framework for the proposed Health and Social Services Access Card (the access card). According to the bill, the access card is intended to:

- Reduce complexity in accessing Commonwealth benefits;
- Facilitate a more convenient, user-friendly and reliable method of accessing those benefits;
- Reduce fraud on the Commonwealth;
- Improve access to Australian Government relief in emergency situations; and
- Permit access card owners to use their cards for such other lawful purposes as they choose.

1.4 The Explanatory Memorandum further explains that the bill:

- Sets out the objects and purposes of the legislation which will form a basis for the uses of the card and a basis for collection, use and disclosure of information on the register and card;
- Provides for the introduction of a new chip-based card to replace the Medicare Card and numerous other cards and vouchers used to access Australian Government benefits;
- Establishes the register and the card to provide certainty as to the information that will be on the register, surface of the card, and in the chip in the access card;

- Introduces a registration process for the card with substantially improved proof of identity arrangements;
- Prohibits unauthorised demands for, and use of, the access card for identity purposes; and
- Vests ownership of the access card in the card holder.

1.5 It is an object of the bill that the access card cannot be used as, or become, a national identity card.

1.6 The bill is the first part of a broader legislative package designed to establish the framework supporting the access card. It has been developed following a consultation process. The bill incorporates many of the recommendations made by the Access Card Consumer and Privacy Taskforce, led by Professor Allan Fels AO.<sup>1</sup> It has also been informed by public comments relating to an exposure draft of the bill, which was released for consultation on 13 December 2006.<sup>2</sup> As part of the continuing legislative process, ongoing consultations on a range of issues, such as the use of the card in dealing with dependents, are being undertaken. The Access Card Consumer and Privacy Taskforce is also continuing its consultations and will provide further advice to the Government.

### **Conduct of the Inquiry**

1.7 The Committee advertised the inquiry in *The Australian* on 12 February, 21 February and 7 March 2007, inviting submissions by 28 February 2007. To help promote awareness of the inquiry, the committee also advertised in the *Australian Financial Review*, the *Sydney Morning Herald* and *The Melbourne Age* on 12 February 2007, and the Chair contacted by way of email the editors of as many news publications as possible, encouraging them to publicise details of the inquiry.

1.8 Sixty-six submissions were received, and these are listed at Appendix 1. Submissions were also posted on the Committee's website to facilitate public access. The Committee held hearings in Sydney on 2 March 2007, in Melbourne on 5 March 2007 and in Canberra on 6 March 2007. A list of the witnesses who appeared at the hearings is at Appendix 2, and copies of the Hansard transcript are available through the Internet at [http://www.aph.gov.au/Senate/committee/fapa\\_ctte/index.htm](http://www.aph.gov.au/Senate/committee/fapa_ctte/index.htm).

---

1 The Taskforce undertook over 160 consultations and received more than 100 submissions. The Government also established an access card website with an email facility, which received over 500 comments from the public; and an access card information hotline which received over 1800 calls.

2 More the 120 submissions from government and non-government organisations, as well as individuals, were received in response to the exposure draft.

## **Acknowledgement**

1.9 The committee appreciates the time and work of all those who provided written and oral submissions to the inquiry, particularly in light of the tight time frame imposed. Their work has assisted the committee considerably in its Inquiry.

## **Note on references**

1.10 References in this report are to individual submissions as received by the committee, not to a bound volume. References to the committee Hansard are to the proof Hansard: page numbers may vary between the proof and the official Hansard transcript.



# Chapter 2

## Overview of the bill

2.1 The Australian government currently provides a range of benefits, services and payments, through different agencies. This bill concerns the services provided by a number of those agencies, referred to as participating agencies.<sup>1</sup> The Government has announced that from 2010, it will be mandatory to be registered and have an access card to claim Commonwealth benefits from those agencies. The bill concerns some of the arrangements under which this system would operate.

### Provisions of the bill

2.2 The main provisions contained in the bill, as described in the Explanatory Memorandum (EM),<sup>2</sup> are set out below.

#### *Registration*

2.3 Part 2 of the bill sets out the arrangements for registering to receive an access card. It explains that there will be a register managed under the authority of the Secretary of the Department of Human Services, and that a person will need to be listed on this register to obtain an access card. A person is eligible to be on the register if they are eligible or qualified for a Commonwealth benefit, are not already registered and are at least 18 or exempted from this requirement.<sup>3</sup> The secretary must provide written notice confirming registration.<sup>4</sup>

2.4 The register will be established separately from existing agency databases, and will not be amalgamated with existing databases. It will not contain medical or health information, or transactional records. Detailed customer records will continue to be held by Centrelink, Medicare Australia, the Department of Veteran's Affairs and other participating agencies. Eligible persons will only need to register once for a service, and only notify participating agencies once of changes in circumstance.<sup>5</sup>

---

1 Participating agencies are the Department of Human Services (including the Child Support Agency, and CRS Australia), the Department of Veteran's Affairs, and the Human Services agencies including Centrelink, Medicare Australia, Australian Hearing Services and Health Services Australia Limited.

2 Most of the text in this chapter is taken directly from the bill, the Explanatory Memorandum to the bill, and the Second Reading Speech.

3 Clause 12, Clause 22.

4 Clause 15.

5 Second Reading Speech, p. 4.

2.5 The information on the register will be verified and will be able to be checked against cards that are presented by individuals when they claim benefits or seek services.<sup>6</sup>

2.6 Information held on the register will include a person's name, date of birth, citizenship or residency status, indigenous status if requested, sex, contact details, benefit card details and registration status. Where the person has an access card, details of that card will also be held, including the access card number, the date the card was issued and its expiry date, a personal identification if there is one, a photograph and a numerical template derived from that photograph, and a digitised signature. If the access card has expired or been deactivated that fact will also be recorded. In addition, the register will include information about the documents used to prove identity, and emergency payment numbers where this is relevant.<sup>7</sup>

2.7 The secretary must not include information about a person where that would be contrary to the person's inclusion in the National Witness Protection Program, or where doing so would be inconsistent with a Commonwealth law.<sup>8</sup> The register must only contain the information specified in the relevant subsections of the bill.<sup>9</sup>

### ***The access card***

#### *Obtaining an access card*

2.8 The bill explains that to obtain an access card after becoming registered, a person must lodge a written application to the Secretary, and where this is approved<sup>10</sup> attend an interview,<sup>11</sup> have a photograph taken and provide a signature, unless exempt from this requirement.<sup>12</sup>

---

6 Explanatory Memorandum, Clause 17, p. 20.

7 Clause 17. For those individuals receiving benefits from the Department of Veteran's Affairs, information about veteran status will also be included on the register.

8 Clause 18.

9 Clause 20.

10 Clause 23. In approving an application form, the Secretary must consult with the Privacy Commissioner and take into account any comments made by the Privacy Commissioner; however, a failure to comply with this requirement does not affect the validity of the approval of the form.

11 Applications will be able to be made at a variety of locations and offices throughout Australia, including existing Medicare and Centrelink offices. Explanatory Memorandum, Clause 23, p. 27.

12 Clause 24. A person may be exempted from having a photograph taken or being required to produce a signature in certain circumstances detailed in section 65 of the bill. For example, persons living in remote Australia, homeless persons, frail persons or persons with a disability, or people at risk may not be required to provide all the specified information.

2.9 As a primary objective of the access card is to prevent fraud, the registration process must be robust and secure. Consequently, during the registration process a person will have to provide certain documents to prove his or her identity. These documents will include such things as birth certificates, passports, immigration documents, and drivers' licenses.<sup>13</sup> Documents will be verified to ensure that forged or duplicate documents are not used to fraudulently register people who are not eligible for an access card.

2.10 The Secretary will issue an access card by post or another method determined by the Secretary, and a person will collect the access card from a designated location.<sup>14</sup>

*Information contained on and in access cards*

2.11 The access card itself will have designated information displayed on its surface. The only mandatory information will be a photograph of the card owner, the owner's name and his or her digitised signature as provided during the interview, and the card's expiry date and number.<sup>15</sup>

2.12 In addition to information on the access card's surface, the access card will contain a chip, divided into the Commonwealth's area and a personal area, where further information will be kept. The Commonwealth's area of the chip will include the same information as the register, and in addition the Secretary may include technical or administrative information (for example, audit logs or the chip's serial number) as long as this information does not identify a person by name or other personal identifier. Similarly, the Minister may include other information in the Commonwealth's area of the chip, as long as that information is only necessary for the purposes of this Act.<sup>16</sup>

*Ownership and use of an access card*

2.13 The access card will be owned by the access card holder, and card owners may use their access card for any lawful purpose they choose. This may include using the access card as a convenient proof of identity document; however, such use is not intended to convert the access card into a national identity card.<sup>17</sup>

2.14 A Commonwealth officer from a participating agency may use an access card only with the consent of the card's owner, and for the purposes of the Act. This

---

13 Explanatory Memorandum, Clause 13, p. 18.

14 Clause 28.

15 Second Reading Speech, p. 4.

16 Explanatory Memorandum, Clause 34, p. 38.

17 Explanatory Memorandum, Clause 40, p. 40-41.

provision is intended to constrain the use of the access card and address concerns about function creep.<sup>18</sup>

### *Offences*

2.15 Section 15.4 of the Criminal Code will apply to offences listed in the bill, and these offence provisions will apply wherever they occur – whether in Australia or not and whether they are committed by an Australian citizen or not. Accordingly, if a foreign national manufactures false access cards overseas, that person will commit an offence against the bill.<sup>19</sup>

#### *Requiring production of an access card*

2.16 There has been some concern expressed about the possibility that businesses would be able to demand the production of the card as a form of identity. A person will be taken to 'require' the production of an access card if they provide no alternative option for a card owner to prove they are who they say they are.<sup>20</sup>

2.17 This bill makes it an offence, punishable by a maximum penalty of five years imprisonment or \$55,000 (or both) for any person – and up to \$275,000 for a company – that requires a card owner to produce his or her card for any purpose except for the provisions of Commonwealth health and social services benefits or to verify concessional status.

2.18 Similarly, it will be an offence for a person to make a copy of, or divulge, a card owner's photograph, signature or card number unless it is for the limited purposes of the Act or with the owner's consent.<sup>21</sup>

2.19 It will not be an offence for a person who is a delegate or an authorised person under the bill to require the production of an access card for identification purposes where that production is for the purposes of the bill. This is a necessary exemption and is consistent with the policy to introduce the card as an effective anti-fraud measure in relation to the delivery of Commonwealth benefits.<sup>22</sup>

#### *Doing things to access cards*

2.20 The bill makes it an offence to intentionally deface or damage an access card belonging to someone else, or a person's own card where this is with dishonest intent. It will also be an offence to intentionally change the information in the

---

18 Explanatory Memorandum, Clause 41, p. 41.

19 Explanatory Memorandum, Clause 44, p. 43.

20 Explanatory Memorandum, Clause 46, p. 45.

21 Second Reading Speech, p. 4-5.

22 Explanatory Memorandum, Clause 45, p. 44.

---

Commonwealth's area of the chip in someone else's card, or in a person's own card where this is with dishonest intent.

2.21 Even though a person may own their access card, the bill makes it an offence for the person to intentionally sell their access card. Similarly, it will be an offence to sell someone else's access card. This is important given that the card is intended to be a major factor in reducing fraud against the Commonwealth, and significant penalties are attached to these offences.<sup>23</sup>

### *Other offences*

2.22 The bill also makes provision for a variety of other offences related to access cards which are designed to safeguard the integrity of genuine access cards.

2.23 In particular, it will be an offence to dishonestly obtain an access card, or to obtain an access card using false or misleading statements, information or documents; to possess a false access card; or to copy an access card number, photograph or signature without authorisation. Any attempt to degrade the anti-fraud aspects of the card warrants significant penalties.<sup>24</sup>

2.24 Similarly, it will be an offence for persons with authority to issue access cards if they know that issuing the card will be contrary to the bill; or to pressure someone else to do so knowing it will be contrary to the bill.<sup>25</sup>

2.25 In view of the importance of the access card to the effective delivery of Commonwealth benefits (including as a fraud prevention measure), the Government believes the name of the card should be protected and not available for use in business. The use of the name in business could cause significant confusion amongst consumers, degrade the integrity of the card and could facilitate the manufacture of misleading cards. For these reasons the Government has decided that the name of the card should vest exclusively in the Commonwealth.<sup>26</sup>

### *Exemptions and delegations*

2.26 The general rule of the bill is that all individuals seeking to obtain an access card will need to follow the same procedures. However, it is recognised there may be times when this is not possible. For example, some individuals may be too ill to attend an interview; some may suffer emotional distress if required to have their photograph taken; or there may be times when it is inappropriate to include a person's residential address in the Commonwealth's area of the chip.

---

23 Explanatory Memorandum, Clauses 47 to 53, pp. 46-50.

24 Explanatory Memorandum, Clause 54, p. 51.

25 Explanatory Memorandum, Clause 61, p. 55.

26 Explanatory Memorandum, Clause 63, p. 56.

2.27 For these reasons, the bill makes it possible for the Minister or the Secretary to exempt persons (other than a Department of Veteran's Affairs (DVA) individual) from the general requirements in appropriate circumstances. A similar power is provided to the DVA Minister and DVA Secretary in relation to DVA individuals. Ministers will be able to exempt certain classes of individuals, while Secretaries will only be able to exempt specific individuals.<sup>27</sup>

2.28 The Ministers and Secretaries will also be able to delegate certain powers of functions to Commonwealth officers in a participating agency in some circumstances.<sup>28</sup>

---

27 Explanatory Memorandum, Clause 65, p. 58.

28 Explanatory Memorandum, Clauses 68-71, pp. 59-61.

# Chapter 3

## Key issues

### Introduction

3.1 This bill is intended to be the cornerstone of the government's proposed access card system. It will provide the legislative basis for the card's roll out, operation and the architecture supporting it. As chapter 2 indicates, the bill's provisions cover a large range of complex matters extending from the purpose of the card through to the information on its surface, chip and database, as well as penalties for misuse. However, at the heart of the proposed access card system are two primary goals:

- Improving delivery of Commonwealth human services and benefits; and
- Combating fraud, particularly in relation to identity theft.

3.2 The Committee endorses goals to streamline the delivery of Commonwealth benefits and prevent fraud. The Committee supports any policy that will facilitate access to those who are eligible while forestalling access to those who are ineligible.

3.3 In considering the bill's provisions, the Committee has used these two goals as a point of reference for assessing the merits and necessity of measures provided for in the bill.

3.4 This chapter examines the following matters in the bill:

- The information to be stored on the card's surface and in its chip;
- The register;
- Discretions and delegations;
- Administrative review;
- Access to the information on the card and in the register; and
- Offences.

3.5 The chapter also lists a number of items of concern that the Committee has not had adequate time to consider.

3.6 To understand the context of the Committee's discussion of the key issues in the bill, it is important to outline a number of timing factors that have shaped the design of the bill, impinged on the Committee's inquiry and which raise concerns about the legislative approach to this measure.

## Timing issues

3.7 The Australian Government submission justifies the timing of the bill on three grounds. Under the heading, 'Why the first instalment of the legislation is needed now', it states:

- A legal framework is needed to support the implementation of the access card system and initial registration of card holders in early 2008;
- It is also needed to allow sufficient time to inform the community about the new system, a step recommended by the Consumer and Privacy Taskforce headed by Professor Fels (and referred hereafter as the 'Fels' Taskforce'); and
- '... early passage of the legislation is required to provide certainty for contract negotiations for the procurement of critical elements of the access card system'.<sup>1</sup>

3.8 The government submission further explains that legislation for the card is being staggered in a series of bills to make it easier for the community to understand the measure, to avoid public confusion which might result from a large, complex omnibus bill and to allow people to focus on specific issues in a considered way.

3.9 The Committee has a number of concerns with the approach and timing adopted with this bill. The most immediate is the limited time given to the Committee to examine the bill, to receive and hear evidence and consider the issues presented to it.

3.10 With only the first tranche of the access card legislation before it, the Committee has also been put at a disadvantage in that it does not know the detail of key provisions and measures that are intended to be addressed in later legislation. That the provisions held over relate to critical matters such as reviews and appeals, privacy protections and oversight and governance measures does little to allay the Committee's general unease with the adequacy of this bill.<sup>2</sup> In essence, the Committee is being asked to approve the implementation of the access card on blind faith without full knowledge of the details or implications of the program. This is inimical to good law-making. The delay in introducing these measures is unlikely to encourage public confidence in the access card proposal, particularly as the missing measures are essential for providing the checks and balances needed to address serious concerns about the bill.

3.11 The Committee has also been asked to consider the bill while a number of processes central to the operation of the access card or of bearing on its legislative framework are still underway. The most important include:

---

1 *Submission 39*, p. 9.

2 The Australian Government submission lists 12 matters not addressed in the first bill which presumably will be covered in subsequent tranches of access card legislation. *Submission 39*, pp 11-12.

- The Fels' Taskforce reporting on the registration process, appeals and a privacy impact assessment;
- The Australian Law Reform Commission's review of the Privacy Act; and
- The Attorney-General's Department's project for a Documentation Verification System.

3.12 In addition, two tender processes, one for the systems integrator, the other for card issuance and management, were running during the Committee's consideration of the matter.<sup>3</sup> This could be seen as undermining the authority of the Committee by creating the impression that passage of this legislation is preordained, rendering Senate oversight superfluous.

3.13 The Committee appreciates that a complex, multifaceted and expensive project like the access card involves several processes running in parallel, and that it is not possible to have answers for every issue or detail during the introductory stages of such an undertaking.

3.14 The government submission has argued that any lengthy delay with the adoption of the bill would hamper the introduction of the access card system. It states:

If passage of the Bill were to be significantly delayed this would reduce the time available to put in place the necessary infrastructure, administrative arrangements and public information to properly implement the new system. This could jeopardise contract negotiations and would not allow adequate time to fully and adequately inform the Australian community of these important changes.<sup>4</sup>

3.15 The Committee cannot accept that priority has been given to tender processes at the expense of reasonable time for the Parliament to scrutinise properly a complex piece of legislation.

3.16 Moreover, the processes surrounding the bill appear to have led to inconsistencies with other Commonwealth legislation and concerns among other Commonwealth agencies. The Committee heard that the bill potentially conflicts with the customer verification obligations under new anti-money laundering and counter-terrorism financing laws.<sup>5</sup> (In subsequent advice, government agencies said they believe this is not the case.)<sup>6</sup> The Australian Federal Police (AFP) also raised concerns

---

3 For a description of both tenders, see *Committee Hansard*, Additional Budget Estimates, 16 February 2007, p. 4.

4 *Submission 39*, p. 9.

5 See Australian Bankers Association (ABA), *Committee Hansard*, 5 Melbourne 2007, Melbourne, pp 53-56. See also ABA, *Submission 52* and Abacus – Australian Mutuals, *Submission 56*.

6 Advice from AUSTRAC (dated and received 14 March 2007) and Department of Human Services, *Answers to Questions on Notice, Questions from Senator Nettle 6 March 2007*, (received 9 March 2007), Question 8, p. 15.

about penalty provisions inhibiting intelligence and investigations.<sup>7</sup> These problems raise questions about the drafting of the bill and degree of consultation among government agencies about the interaction of the bill with other Commonwealth law.

3.17 Legal academics and practitioners also criticised the bill for its poorly defined terminology and other drafting deficiencies. While committee scrutiny of bills is designed to identify and fix problems of this nature, the limited time allotted means other problems may go undetected while any remedial amendments will also have to be rushed and risk further drafting inconsistencies.

3.18 The haste involved with this bill has also led to a number of irregular and inappropriate actions. The department published on its website the Australian Government submission to the inquiry before the Committee could consider its contents, let alone authorise its publication. This breached the longstanding rule and practice that Senate committees have sole discretion to publish evidence they receive. The Committee also received evidence from the department that did not take account of other powers and procedures of the Senate and its committees (for instance, in relation to claims of legal professional privilege). The Committee assumes these oversights were largely a result of the haste with which this inquiry has had to be prosecuted.

### *Conclusions*

3.19 The time allowed for consideration of all the important and complex issues relating to the access card legislation has been truncated, including the time given to the Committee to examine this bill. Key measures that need to be taken into account including privacy, governance, appeals and review mechanisms are to be considered in a second tranche of legislation. It is not possible to assess adequately this new measure in the absence of these vital protections and other provisions. The Committee considers that this bill needs to be combined with the second tranche of legislation into a consolidated bill to allow proper consideration of the access card proposal.

### **Recommendation 1**

**3.20 The Committee recommends that this bill be combined with the proposed second tranche of legislation for the access card system into a consolidated bill.**

### **The Card – surface information**

3.21 In seeking to explain how the primary objectives of improved service delivery and fraud prevention will be met, the bill includes provisions for what information will be displayed on the surface of the card and in the chip inside the card. Clause 30 of the bill states that information displayed on the surface of the card will include,

---

7 *Committee Hansard*, 6 February 2007, Canberra, pp 6, 10.

among other things, the cardholder's photograph, and the cardholder's signature, and the access card number.<sup>8</sup>

3.22 The sections below discuss the case for these features and the concerns raised about them.

### *The photograph*

3.23 In its written submission to the inquiry, the Australian Government stated that including a photograph on the surface of the card is essential to the integrity of the new scheme, as 'The inclusion of a photograph on the card will significantly enhance the identity security elements of the card, protecting the card owner's identity and reducing opportunities for fraud'.<sup>9</sup>

3.24 The Office of Access Card elaborated on this by noting that the inclusion of a photograph on the surface of the card would be essential to:

- reduce fraud;
- reduce complexity;
- increase customer convenience;
- provide a user friendly and reliable method for accessing Commonwealth benefits;
- improve access to Australian Government relief in emergency situations; and
- permit access card owners to use their access cards for such other lawful purposes as they choose.<sup>10</sup>

3.25 It also highlighted the importance that government agencies place on the photograph for combating fraud. The Office of Access Card provided material from the Australian Federal Police (AFP) stating that the AFP's operational experience has shown that:

...in cases of systematic and organised identity fraud, the one single feature that remains constant in offenders is their facial features. This highlights the necessity and importance of having a facial photograph...The proposed Access Card regime provides greater surety of the link between an individual and relevant entitlements through the enhanced security features, and also protects the individual. The presence of a photograph on the surface of the card provides a basic verifiable link to the person claiming the entitlement, benefit or service.<sup>11</sup>

---

8 *Human Services (Enhanced Service Delivery) Bill 2007*, clause 30, page 31. See also *Explanatory Memorandum*, pp 32-33.

9 Australian Government, *Submission 39*, p. 33.

10 Department of Human Services, *Submission 39a*, p.1.

11 Department of Human Services, *Submission 39a*, pp 2-3.

3.26 The Office of Access Card further stated that:

Without a photo on the surface of the card it will always be the case that people will be able to get someone else's entitlements as photographic readers will not be available everywhere, every time.<sup>12</sup>

3.27 By contrast, it claimed that putting the photograph on the surface of the card will be a major deterrent to people considering defrauding the system:

KPMG has noted that it takes considerable bravado to walk into a doctor's surgery and present a card with someone else's photo on it.<sup>13</sup>

### ***Concerns about including a photograph on the surface of the card***

3.28 Four general arguments were presented to the Committee that raised doubt about the necessity for the photo to be on the card's surface. The following section looks at each of these in turn.

#### *The access card as a national identity card*

3.29 Any consideration of the proposal to show a personal identifier such as a person's photograph on the card's surface needs to examine the question of whether the access card might become a national identity card. Frequent references arose in evidence about the parallels between the proposal for the access card and an earlier proposal for a national identity card. This issue goes to the heart of the bill's objectives and rationale. It also goes to the heart of concerns about the privacy implications of the access card system. As such, the Committee considers that the case for constructing the card with or without certain features must be sound and properly tested.

3.30 Some witnesses and submissions suggested that the inclusion of personal information, particularly a photograph on the card's surface, represents the greatest risk of the card becoming a *de facto* national identity card. The Australian Privacy Foundation stated that:

... if all of that information can be read off the chip, there is no need to have it on the surface of the card for the objective of the card. By having it on the surface of the card when it is not needed for that objective, it lends the card more weight as an all-purpose ID card and means banks, Video Ezy et cetera will want to see it.<sup>14</sup>

3.31 Similarly, the New South Wales Council for Civil Liberties submitted that:

The Access Card will be readily capable of use as an identity card because it will carry on its face five pieces of identity information: a unique id

---

12 Department of Human Services, *Submission 39a*, p. 3.

13 Department of Human Services, *Submission 39a*, p. 4.

14 Ms Johnston, *Committee Hansard*, 2 March 2007, p. 21.

number; a name; a date of birth; a photograph; and a signature...An id card is an undesirable thing in a free society that promoted civil liberties. It unreasonably provides to the State a tool with a range of potentially oppressive uses...The id number, photograph and signature need not appear on the face of the card. Recording them on a secure area of the chip, accessible only by authorised persons, would resolve this aspect of the proposal.<sup>15</sup>

3.32 The Government has given assurances that the access card is not intended as a national identity card.<sup>16</sup> The Committee is concerned, however, that not enough attention has been given to the practical effect of information on the surface of the card.

3.33 In this regard, the Committee has taken particular note of the Taskforce's view that:

...most Australians are eligible for Medicare, so even those who do not make regular use of Medicare services are likely to find that at some time in their lives, for example when they start a family or when they reach a certain age or degree of infirmity, they will need to access Medicare. To do so they will need an access card. To this extent, the Taskforce recognises that, at some stage, *almost every Australian* is likely to need an access card and as such to become a person registered in the Secure Customer Registration Service.<sup>17</sup> [italics added]

3.34 The Committee remains concerned that the inclusion of a biometric photograph, as well as the other information on the surface of the card, could trigger public concern about the access card becoming the preferred identity document of most Australians. There is no comparable document issued on a national scale in Australia that contains a photo of biometric quality.

3.35 Alternative forms of identity are not likely to be considered as authoritative, for example, drivers' licenses are issued by states rather than the Commonwealth, and the photos that appear there are of non-biometric quality. Passports are not issued on a universal basis, and their bulky size guarantees that they will not be routinely carried by most citizens.

---

15 *Submission 29*, p. 3. See also, for example, Access Card No Way Campaign, *Submission 41*, p. 5.

16 The Government has stated that the card will not be a national identity card; will not be compulsory for every Australian; will not be an electronic health record; will not record your financial details; will not be required to be carried at all times; will not be required to transact normal everyday business; will not be required to be shown to anyone other than for the provision of health and social services benefits provided by the Australian Government and to confirm concession status. Human Services (Enhanced Service Delivery) Bill 2007, *Second Reading*, p. 2.

17 Consumer Access and Privacy Taskforce, *Discussion Paper Number 1: The Australian Government Health and Social Services Access Card*, 15 June 2006, pp. 18-19.

*Semantic imprecision*

3.36 The imprecise wording of key items in the bill raised further concerns that there are inadequate constraints to prevent the access card becoming an identity card.

3.37 For instance, a 'Commonwealth Benefit' is defined in the clause 5 of the bill as a 'benefit or service that:

- a) is provided to an individual (whether under Commonwealth law or otherwise);  
and
- b) is administered or delivered, wholly or partly, by a 'participating agency'".

3.38 However, the wording of this definition suggests that any concession granted by virtue of veteran or pensioner status could be deemed by the wording of this definition to be a 'Commonwealth Benefit' because one of the specified 'participating agencies' will be involved as a gatekeeper in determining eligibility for the benefit. This could be deemed to satisfy the 'administered or delivered, wholly or partly' definition in clause 5.

3.39 The possibility of function creep may be increased by clause 7 of the bill stating that the purposes of this bill:

...are to facilitate the provision of benefits, services, programs or facilities to some or all members of the public (whether under Commonwealth law or otherwise), where that provision involves a participating agency.

3.40 The language of this clause could conceivably allow the providers of state concessions to claim inclusion in the provisions of this bill. The 'benefits, services or facilities' are to be provided to 'some or all members of the public'. The provision of these benefits is to be authorised by 'Commonwealth law, or otherwise'. As long as a participating agency is 'involved,' regardless of how peripherally, the service or benefit could be construed to come within the ambit of the bill. For example, the DVA's 'gatekeeper' role in the provision of concession status to veterans might allow public transport providers (for instance, the NSW railways) to make such a claim.

3.41 The expansion of Commonwealth benefits status to State and Territory concessions would further enhance the ubiquity of access card usage, and would materially contribute to its emergence as the dominant identity document in day to day use throughout Australia.

3.42 Thus, it is argued that there is potential for the access card to evolve into an ID card if a biometric photo, signature and serial number are visible on the face of the card. However, this might contravene the government's explicit declaration in clause 6 (2) that 'access cards are not to be used as, and do not become, national identity cards'.

3.43 The Committee remains mindful of public concerns that the inclusion of a photograph on the surface of the card could lead it to become Australia's *de facto* ID card, and that this conflicts with the stated objectives of the bill.

---

*The necessity of the photograph for improved service delivery*

3.44 Enhanced service delivery is one of the key objectives of the bill. The function of a photograph in this regard was noted by Professor Allan Fels during public hearings:

There would be quick recognition of them (the card holder) in dealings with the government and maybe in dealings with doctors, pharmacies and so on. It is the idea that you just hold up the card and it shows your face. If you did not have the photo on the card, I think whoever was dealing with you, the cardholder, would have to take a bit of time to look you up.<sup>18</sup>

3.45 However, the use of card readers to determine eligibility for services has cast doubt in some witnesses' minds on whether the photograph is necessary on the card's surface. Since readers would show the person's photograph on the card's chip, the need to have the photograph on the card's surface would not appear to be essential or mandatory. Professor Fels told the Committee:

...the big thing for them is to have a photo in the chip and on register, rather than necessarily compelling it to be on the card when there would be some people who would be strongly opposed to that and not like it and there would be others who, given the choice, would not want their photo on it.<sup>19</sup>

3.46 On this basis, Professor Fels concluded that it would be preferable for the inclusion of a photograph on the surface of the card to be a matter of individual choice:

...I now tend to see the idea of it being a matter of choice as having a lot of merit, almost to the point where I think a very strong case would need to be made against that before you would remove the consumer choice possibility.<sup>20</sup>

3.47 Similarly, the Privacy Commissioner expressed her preference that the inclusion of a photograph on the surface of the card be a matter of individual choice.<sup>21</sup>

3.48 However, the Office of Access Card informed the Committee that not all service providers would have card readers capable of viewing the photograph in the chip:

While the Human Services' agencies will have the capability, doctors, pharmacists, allied health professionals, specialists, hospitals and third party concession providers will not. To introduce another card reader into a

---

18 *Committee Hansard*, 6 March 2007, p. 59.

19 *Committee Hansard*, 6 March 2007, p. 60.

20 *Committee Hansard*, 6 March 2007, p. 60.

21 Ms Curtis, *Committee Hansard*, 6 March 2007, p. 36.

doctor's surgery or a pharmacy will impose an unacceptable burden on their business.<sup>22</sup>

3.49 The Office's supplementary submission, received very late in the inquiry process, went on to note that the photograph on the surface of the card is central to flexible service delivery, which is important given the wide range of service delivery models which exist within Human Services, and that providing alternative photographic identification is not ideal for reasons relating to security, privacy and customer convenience.<sup>23</sup>

3.50 The supplementary submission further asserts that the cost of supplying photo capable readers to all service providers would be \$15 million (50,000 units costing \$2,500 per unit).<sup>24</sup> The cost of upgrading terminals to photo capable status would cost an additional \$700 million.<sup>25</sup> The Committee was provided with no detailed information to support these cost estimates.

3.51 However, assuming that they are accurate, they do nothing to detract from the primary issue relating to the access card photograph – the inclusion of a photo on the face of the card virtually guarantees its rapid evolution into a widely accepted national form of identification.

3.52 The Committee considers that even if the costs involved are quite substantial, fiscal considerations of investment in public infrastructure (such as readers) should not necessarily trump privacy and civil liberties concerns on the question of the access card photograph.

#### *Impact on service providers*

3.53 The Committee was also told that including a photograph on the surface of the card, with the expectation that it will allow service providers to quickly verify a card holder's identity, may transfer the burden of assessing eligibility to individual service providers rather than government agencies. The Australian General Practice Network (AGPN) submitted that:

AGPN is supportive of ensuring that only eligible patients are able to access the government rebate; however the quantum of any fraud and the extent of disputes/conflict that arise on eligibility grounds will now be more prevalent in the practice. This increased scrutiny is not something that practices are currently funded for or trained to cope with, particularly as GPs do not ration care on the basis of eligible/non-eligible Medicare guidelines; rather they seek to improve the health outcomes of any person that requires treatment or advice. The proposed approach passes the

---

22 Department of Human Services, *Submission 39a*, p.1

23 Department of Human Services, *Submission 39a*, p. 9.

24 Department of Human Services, *Submission 39a*, p. 11.

25 Department of Human Services, *Submission 39a*, p. 11.

---

responsibility of managing the physical process for checking a patient's eligibility to access an Australian Government rebate to the practice without acknowledging this in the legislation.<sup>26</sup>

3.54 The Committee is concerned that the AGPN's comments reflect a lack of information about the training and other assistance which will be given to service providers to manage situations involving improper use of the card.

*Risks of counterfeiting*

3.55 To put the question of the photograph and fraud in perspective, the Committee was concerned about the risk of the access card being counterfeited and whether including a photograph on the card may support fraudulent activity by providing an extra layer of legitimacy to false identities.

3.56 With regard to counterfeiting, one witness suggested:

...I think there are vast commercial opportunities available to a whole lot of people in shady alleys as a result of this who will be selling lovely copies of the plastic of the ID, for example, to go down to your local video store, which will not have a reader, and show them a fake version of an ID card. There are great commercial opportunities that are going to grow with that.<sup>27</sup>

3.57 Another witness referred the Committee to concerns expressed by government figures about the risk of counterfeiting:

In fact, at the Australian smartcard summit on 29 June 2005, the Attorney-General said that a national ID card 'could increase the risk of fraud because only one document would need to be counterfeited to establish identity'. This was supported by the Commissioner of Taxation, who warned that the access card proposal, if implemented, was likely to lead to a rise in identity theft. It is just naïve to assume from the moment that this was proposed there was not already an industry being put in place to produce its own identity cards. If the government can make it, criminals can also copy it. So it does not actually support the case that it will combat identity fraud.<sup>28</sup>

3.58 The Committee is concerned that a lack of information about the risk of counterfeiting, and the possibility of false identities being entrenched and widely disseminated through inclusion of photographs on the card surface, makes it difficult to judge the extent to which the bills' objective of combating fraud will be achieved.

3.59 While the access card's security features appear stronger than the current Medicare card, it cannot be assumed that it will not be vulnerable to corruption and misuse. The question of the risk of counterfeiting the access card needs to be included in any assessment of the card's impact in countering fraud.

---

26 Australian General Practice Network, *Submission 12*, p. 4.

27 Mr Warner, *Committee Hansard*, 5 March 2007, p. 18.

28 Ms O'Rourke, *Committee Hansard*, 5 March 2007, p. 64.

## **Conclusions**

3.60 The Committee concludes that decisions about information displayed on the surface of the card must be informed by the two stated major objectives of the bill: facilitation of access to health and social services, and reduction of fraud against the Commonwealth. While it is recognised that certain groups of people may also find the card to be of convenience for accessing concessions, these are ancillary issues and should not be used to justify the architecture of the access card system.

### *The photograph*

3.61 On the basis of the evidence, the Committee has concluded the inclusion of a biometric photograph on the surface of the card increases the likelihood of the access card becoming a *de facto* national ID card. It is noteworthy that it may not be necessary that the photograph should appear on the surface of the card for the purpose of providing Government services if the providers have access to appropriate card readers.

3.62 The Committee notes the Department of Human Services' supplementary submission which states that there would be considerable cost involved in providing terminals capable of reading the card to agencies, doctors, pharmacies and third party providers. However, the Committee considers that the cost of investing in public infrastructure is offset by the protection of essential privacies and freedoms, and that these should be balanced appropriately. The Committee considers that the government should consider providing appropriate terminals or readers to those agencies and providers providing benefits and services to access card holders.

**3.63 The Committee considers that the government should take the following matter into consideration when drafting the consolidated bill:**

**Whether the government consider providing appropriate terminals or readers to those agencies and providers providing benefits and services to access card holders.**

### *The signature*

3.64 The Committee does not consider that the inclusion of a digitised signature on the surface of the card is necessary to achieve the bill's two key objectives when it is also held in the card's chip and on the register. The main rationale for mandatorily including the signature (that it will facilitate identity assurance where a card holder is not present) is weakened when it is recognised that agencies providing benefits in the absence of a card holder will also have access to data in the Commonwealth's area of the chip, through which a signature on a form may be verified.

3.65 Professor Fels told the Committee that including the signature on the card would mean:

It is one more piece of centrally stored data, and one should exercise a bit of caution and be satisfied that there is a reasonable case for actually having

---

stored somewhere millions of signatures. I think there are some reasonable arguments for making this a matter of choice.<sup>29</sup>

3.66 Similarly, the Committee heard the Privacy Commissioner's view that 'the individual should also be able to choose whether their photo and their signature are displayed on the face'.<sup>30</sup>

3.67 The Committee also noted, however, that there may be circumstances, generally relating to particular card holder groups, in which the inclusion of a signature on the surface of the access card could be helpful in verifying a card holder's identity. The Office of Access Card's supplementary submission noted that some Department of Veterans' Affairs (DVA) benefits are provided in the veteran's home, and that:

The veterans' community was particularly in strong favour of retaining the digitised signature on the surface of the card to enable the transaction of their unique benefits.<sup>31</sup>

3.68 In these circumstances, having a signature displayed on the surface of the card will add another element of surety to verification of a card holder's identity. The Committee considers that the best way of resolving this tension is to make the inclusion of a digitised signature on the surface of the card a matter of choice for individual card holders.

#### *The card number*

3.69 In relation to inclusion of the card number on the surface of the card, the Committee noted the evidence given by Professor Allan Fels which highlighted the relationship between having the number on the card and having a unique personal identifier, and that business methods may be adapted to privacy concerns, rather than the reverse.<sup>32</sup> Professor Fels told the Committee that:

We originally leant against the idea of a number being on the card, but we see much merit in the idea that it is the option of the card holder whether or not there is a number on their card.<sup>33</sup>

3.70 The Committee considers there is a balance to be struck between privacy protection and increased convenience, and concurs with Professor Fel's view that this is best achieved through allowing individual card holders the choice of having their number included on the card surface or not.

---

29 *Committee Hansard*, 6 March 2007, p. 58.

30 Ms Curtis, *Committee Hansard*, 6 March 2007, p. 36.

31 Department of Human Services, *Submission 39a*, p. 19.

32 Professor Allan Fels, Consumer Access and Privacy Taskforce, *Committee Hansard*, 6 March 2007, p. 57.

33 *Committee Hansard*, 6 March 2007, p. 57.

3.71 The Committee is aware that some Australians will choose to forego certain privacy protections in favour of the convenience offered by the access card. It is also mindful of the fact that personal opinions on the balance of privacy versus convenience are likely to evolve over time, with individuals choosing to include or exclude different items of personal information on the card at different times.

**3.72 The Committee considers that the government should take the following matter into consideration when drafting the consolidated bill:**

**Whether the only mandatory information displayed on the surface of the card should be the card holder's name and that other information should be at the discretion of the card holder.**

### **The chip inside the card**

3.73 A number of concerns were raised about the chip inside the proposed card. Some witnesses and submissions claimed there is a lack of clarity about the rationale for having a personal area on the chip. They were also concerned about the bill's silence on what information would be stored in the personal area and how it would be protected and managed.<sup>34</sup>

#### ***The personal area of the chip***

3.74 In particular, concerns have been raised about the suggestion that sensitive health information may be held in the personal part of the chip and be available to health professionals in certain situations, such as emergencies. This issue was covered in a discussion paper released by the Access Card Consumer and Privacy Taskforce on 21 February 2007,<sup>35</sup> which favoured the inclusion of minimal necessary medical information in the chip, accompanied by a robust system of authentication and verification. The Taskforce also noted that:

To be of any use, the data must be readily and easily accessible. This means that anyone with an approved reader...will necessarily be able to view it...As such, card holders who choose to make use of this system must accept that they are putting sensitive personal information, effectively, into the public domain...<sup>36</sup>

---

34 See, for example, ACT Government Chief Minister's Department, *Submission 28*, pp 6-7.

35 Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 2: Voluntary Medical and Emergency Information*, 21 February 2007. The report made nine recommendations, and noted that the storage of personal emergency and medical data on the card differed from other data storage issues in that the card holder does so on an understanding that the data is there to be used by third parties, primarily for the assistance of the card holder themselves. Third parties therefore have an interest in the integrity of the data, and it must be ensured that the operation of such a system must be in accordance with the (competing) priorities of all parties.

36 Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 2: Voluntary Medical and Emergency Information*, 21 February 2007, p. 6.

3.75 This issue highlights the question of achieving a balance between protecting privacy and providing some private details which could be of vital importance in life-or-death situations.

### ***The Commonwealth's area of the chip***

3.76 Discussion of the Commonwealth's area of the chip highlighted the interface between information held there, information held on the register and information held in individual agency databases. There was concern about the data sharing arrangements between these holdings, and whether privacy would be adequately protected. This is discussed later in the section on the register.

3.77 The ability of numerous agencies and individuals to access information in the card by using the card's identifying number also raised privacy concerns. It was suggested that the use of a single identifying number by multiple agencies and individuals encourages the possibility of the card becoming a *de facto* national identity card, and facilitates unauthorised access to a wider range of personal information. The Privacy Commissioner told the Committee that:

This creates a situation where more than one agency can hold a common government issued identifier for a single individual. The risk here is that the ease of matching those records may in the future increase the temptation to change existing restrictions on information sharing between agencies and thus the framework for large-scale data matching could be in place.<sup>37</sup>

3.78 The Committee heard that a possible solution to this problem could be to store existing agency identifiers in the Commonwealth part of the chip, so that when an individual docked a card at an agency the *agency* number rather than the access card number would be identified. The Privacy Commissioner told the Committee that:

I believe that information that may be necessary for a particular agency to determine whether a benefit is payable to an individual should be kept in the individual's record with that agency rather than attempting to establish a central point from which identity verification and eligibility for benefits and services can be determined.<sup>38</sup>

3.79 The proposed arrangement would satisfy the objectives of the bill to facilitate access to health and welfare benefits, while protecting an individual's access card number and private information across different databases.<sup>39</sup>

---

37 Ms Curtis, *Committee Hansard*, 6 March 2007, p. 35.

38 Ms Curtis, *Committee Hansard*, 6 March 2007, p. 35.

39 Ms Curtis, *Committee Hansard*, 6 March 2007, p. 35.

## **Conclusions**

3.80 The Committee acknowledges concerns about the lack of information in the bill regarding the personal area of the card and considers this issue must be dealt with as a priority.

3.81 In relation to sensitive health and medical information being placed on the personal area of the chip, the Committee concurs with the Access Card Consumer and Privacy Taskforce's observation that this issue highlights the balance which needs to be struck between maintaining personal privacy and making information available for the wellbeing of the card holder. The Committee concludes that the question of what information should be placed on the chip is most appropriately left to the discretion of individual card holders, in consultation with medical staff.

3.82 The Committee also notes suggestions from the Privacy Commissioner that the bill's objective of facilitating access to health and social services and welfare benefits, while protecting a card holder's personal information held in different databases, could well be achieved by storing existing agency identifiers in the Commonwealth area of the chip. The Committee supports examination of this option as a matter of priority.

**3.83 The Committee considers that the government should take the following matter into consideration when drafting the consolidated bill:**

**Whether the Commonwealth area of the chip should store existing agency identifiers and that these numbers should be used when linking a card to a participating agency database, rather than the access card number.**

## **The register**

3.84 Personal information about access card holders will be recorded during a registration process and stored on a database known as the register. Clause 16 of the bill requires the secretary to establish and maintain the register. Clause 17 specifies the information to be stored in it.

3.85 The register will be a single database storing basic identity information – name, date of birth, citizenship or residency status and so on – including a photograph and numerical template of a person's photograph as a security and verification measure. It will also include the card holder's digitised signature if it appears on the surface of the card.

3.86 The department stated the register would not amalgamate personal information stored on other government databases, which would continue to be maintained separately by other agencies. It emphasised the register would not be a 'mega database containing health, veterans' and social service records'.<sup>40</sup> Instead, the

---

40 *Submission 39*, p. 19.

register is intended to provide basic information necessary for the payment of health benefits, veterans' and social services delivered by or on behalf of the following participating agencies:

- Centrelink
- Medicare Australia
- Australian Hearing Services
- Health Services Australia Ltd
- Department of Veterans' Affairs (DVA) and
- Department of Human Services (DHS) including the Child Support Agency and CRS Australia.

3.87 The department stated the register would not include or connect to taxation records, census data or personal or financial records.<sup>41</sup>

3.88 The department's explanation of the reason for establishing a centralised data system indicated that this avoided the need to amalgamate data from participating agencies:

The Register is designed to sit as a secure gateway between the card and the specific agency databases. Having a centralised register with only the minimum necessary amount of customer registration data avoids the need to integrate the data of all the participating agencies.<sup>42</sup>

3.89 Despite these assurances, the register, along with the issue of the photo on the card's surface discussed above, is the most contentious element of the access card system. The register gives rise to the prospect of the government having unprecedented access to a single national database containing the majority of Australia's adult population's basic personal information. It is seen as presenting a major risk to personal privacy and security, not only from government agencies but also other parties with malicious intent. The Fels' Taskforce put the significance of the register into historical perspective:

No previous Australian government, even in wartime, has effectively required all its citizens to give it a physical representation of themselves, nor contemplated having this stored in one national database.<sup>43</sup>

3.90 In evidence to this inquiry, the main concerns about the register related to:

- the potential for the register to be used as a national identity base, by virtue of its centralisation of vital personal information for most Australians;

---

41 *Submission 39*, p. 19. See also Department of Human Services, *Answers to Questions on Notice, Questions from Senator Nettle 6 March 2007*, (received 9 March 2007), Questions 9 and 10, pp 16-17.

42 *Submission 39*, p. 71.

43 *Access Card: Consumer and Privacy Taskforce, Report Number One*, September 2006, p. 28.

- access to the register, including by non-participating agencies (such as security bodies and police) and non-authorised access by either government staff or hackers;
- the amount of personal information to be stored in the register;
- the vulnerability of the register to external hacking;
- the discretion provided in the bill to the secretary and minister; and
- the absence of Parliamentary scrutiny or disallowance.

3.91 The question of access is interconnected with concerns that the register will gradually assume greater importance, leading to function creep and its growing use as an identity system. The issues of access and discretion are dealt with later in this chapter.

### ***Personal information concerns***

3.92 A major concern in evidence is that the register will store a range of private information that would leave people at risk if the information were to fall into the wrong hands. This concern relates particularly to the storage of people's addresses and proof of identity documents. Ms Versey, the acting Victorian Privacy Commissioner, pointed to the dangers this information potentially poses to people's privacy and identity:

My specific concerns are that you will now have a register where identity documents, such as birth certificates, are now copied onto the register. This makes it a very rich source for those that want to indulge in identity theft or want to take over identities...

... The less you have on the register the better. If you have a source where you not only have all this personal information but also actually have copies of the identifying documents themselves, then you have the whole person's identity all in one place.<sup>44</sup>

3.93 Other witnesses suggested the inclusion of proof of identity (POI) documents in the register provides the 'raw materials' for identity theft.<sup>45</sup>

3.94 A related concern is that, unless protected adequately, details about people's address could leave them at risk of personal harm if this information leaked out of the system.<sup>46</sup>

3.95 Concerns about the concentration of vital personal data in one database also tie in with fears about the security of the system in which the information is stored.

---

44 *Committee Hansard*, 5 March 2007, Melbourne, p. 4.

45 Australian Privacy Foundation, *Submission 30*, p. 3.

46 Ms Versey, *Committee Hansard*, 5 March 2007, Melbourne, pp 5-6.

## ***Security concerns***

3.96 Several witnesses claimed the establishment of a single repository of personal information would become a target or 'honey pot' for identity fraud and privacy invasion.<sup>47</sup> This gave rise to fears that the vast pool of personal information in the register would be vulnerable to external hacking, on the ground that no information system is entirely secure.<sup>48</sup> Professor Greenleaf of the Cyberspace Law and Policy Centre summed up these concerns:

The collection together of photograph, signature and an undefined range of POI [proof of identity documents] create a system which is an exceptionally high security risk for identity fraud from unauthorised access...<sup>49</sup>

3.97 The Fels' Taskforce recognised that the security of personal information held on the register is of the utmost importance, especially for gaining public confidence and trust in the access card system. Ensuring the photographic database could not be hacked was particularly important in this regard.<sup>50</sup>

3.98 The department's evidence indicates it has a high degree of confidence and faith in the security measures designed to protect information stored in the register. It described the register's anti-hacking architecture as using segregated or 'siloe'd' databases for different items of personal information:

To protect customer information, data in the access card system is not held centrally in one place. No single officer will be able to access all components of the system. The system is modular in design and comprises separate databases (i.e. Secure Customer Database, Photo Database, Biometrics System, Card Management System.) Hackers would be confronted by multiple defences – isolated separate databases protected by many different levels of security and encryption. Any attempt to hack the card would not result in access to the system or any part of the system.<sup>51</sup>

3.99 Even if these security measures are currently robust, it is likely that future technological advances will present both opportunities to enhance the system's security but also pose threats to it. The Committee reaffirms the view of the Fels' Taskforce that the security of the register's information should remain an ongoing priority of the department and agencies supporting it.

---

47 Access Card No Way, *Submission 41*, p. 3; Cyberspace Law and Policy Centre, *Submission 43*, Attachment, p. 3. See also Ms Versey, acting Victorian Privacy Commissioner, *Committee Hansard*, 5 March 2007, p. 2.

48 Australian Privacy Foundation, *Submission 30*, p. 3. Public Interest Advocacy Centre, *Submission 44*, p. 7.

49 *Submission 43*, Attachment, p. 4.

50 *Access Card: Consumer and Privacy Taskforce, Report Number One*, September 2006, p. 34.

51 *Submission 39*, p. 57. See also Department of Human Services, *Answers to Questions on Notice, Questions from Senator Nettle 21 February 2007*, (received 9 March 2007), Question 69, p. 3.

3.100 The Defence Signals Directorate (DSD) is providing advice on the security design of the system and will evaluate and certify its security aspects. DSD will also test the security of system both before and after the system is implemented.<sup>52</sup>

3.101 Professor Fels told the Committee he would be satisfied if DSD approved the system after testing it. However, he also suggested that a twin-pronged approach combining technological and legislative safeguards may be the best guarantee of the system's security.<sup>53</sup> The Committee examines the issue of legislative measures in the next section.

### ***Absence of parliamentary scrutiny or disallowance***

3.102 Clause 16 provides for the secretary to establish and maintain the register in any form or manner the secretary considers appropriate. The explanatory memorandum states it is proposed to keep the register in electronic form. Clause 16 (3) makes the register not a legislative instrument on the ground that it is 'administrative in character'. This means the form and manner in which the register is kept will not be subject to Parliamentary oversight or disallowance.<sup>54</sup>

3.103 The Office of the Victorian Privacy Commissioner encapsulated concerns over the absence of Parliamentary scrutiny or disallowance in relation to both the maintenance of the register and the information kept on it. It noted that the explanatory memorandum says the register will be kept separate from databases maintained by other participating agencies and there will be no centralised database holding all of a person's information in one place, but that the bill does not expressly prohibit this. It went on to say:

The form and manner in which the Register is to be kept will have a significant impact on the privacy interests of individuals and the necessary security and other safeguards that must be considered and established. This should be set out in legislation and prohibitions such as keeping the Register separate from other data bases expressly stated.<sup>55</sup>

3.104 The Fels' Taskforce was also of the view that to enhance public support for the access card scheme and win acceptance of it, decisions related to the register should be reviewable by the Parliament.<sup>56</sup> Professor Fels told the Committee that in considering the question of safeguards:

---

52 *Submission 59*, p. 2. See also the discussion of security in *Access Card: Consumer and Privacy Taskforce, Report Number One*, September 2006, p. 58.

53 *Committee Hansard*, 6 March 2007, p. 63.

54 Explanatory Memorandum, p. 20.

55 *Submission 48*, p. 5.

56 Consumer and Privacy Taskforce, submission on the exposure draft of the bill, p. 2.

---

... I would suggest that one should err on the side of caution in this matter in terms of maximising the parliamentary review processes and appeals and so on.<sup>57</sup>

3.105 The Committee also notes Professor Fels' view that parliamentary oversight could complement technical measures to strengthen the security and governance of the register.

3.106 Establishing an ongoing Parliamentary role in overseeing the register would provide a channel for any community concerns to be raised and ensure transparency over the way in which the register is maintained. In this regard, it would also allow the Parliament to monitor the ongoing security of the register and provide a safeguard in the event of security problems or any expansion of the register's purpose arising. This would provide a significant measure for maintaining public confidence in the access card system.

### ***Conclusion***

3.107 The establishment of the register is a new measure of national significance with far reaching implications for the privacy and security of most Australians' personal data. It is vital that the necessary level of transparency and oversight is also established to monitor its use. The current bill does not provide these necessary mechanisms.

3.108 The legislation should provide for Parliamentary scrutiny of the maintenance of the register and review of any decisions to alter the manner and form in which it is kept or the personal information to be recorded in it. The bill should also stipulate that the register will be kept separate from other agency databases (both participating and non-participating agencies) and there will be no centralised database holding all of a person's information in one place.

**3.109 The Committee considers that the government should take the following matter into consideration when drafting the consolidated bill:**

**Whether the form and manner in which the register is to be kept should be set out in legislation and prohibitions such as keeping the register separate from other data bases should be expressly stated.**

### **Discretions and Delegations**

#### ***Discretions***

3.110 Liberty Victoria identified 29 separate discretions that are vested in the minister by the bill, which include 23 discretions vested in the secretary that are subject to ministerial direction under Clause 8 of the bill. According to that witness many of these discretions affect the operation of the Bill in fundamental ways, e.g.

---

57 *Committee Hansard*, 6 March 2007, pp 61-62.

those permitting certain persons not to register and those affecting the information which must be provided for proof of identity, for inclusion on the register and for inclusion on the card.<sup>58</sup>

3.111 It was alleged that these and other non-reviewable provisions would facilitate 'function creep' by providing for discretions in the secretary and minister to make decisions that would expand the system, but that would be not disallowable by Parliament.<sup>59</sup>

3.112 At a more fundamental level there is also a concern that the bill 'vests extraordinarily wide discretions in both the Minister and the Secretary of the Department of Human Services, which are tantamount to a delegation of legislative power to them'.<sup>60</sup>

3.113 Such statements might lead to the conclusion that the bill would grant the minister and secretary unfettered discretion in all matters.

3.114 Some discretions are to be exercised by way of legislative instruments that are disallowable. These include discretions that would allow the minister to add personal information to the register or to the Commonwealth area of the chip (Clauses 17(1)(17)(b) and 34(1)(17)(b)). The bill also requires the minister to determine guidelines that must be taken into account by the secretary when making certain decisions relating to applications and registration by way of a disallowable legislative instrument (Clause 66).

3.115 However, even these provisions are contentious. For example, the Government submitted that the secretary would not have the power to add personal information to the Register and that only the minister could do that by disallowable legislative instrument.<sup>61</sup> The Cyberspace Law and Policy Centre (CLPC) argued, however, that the secretary would have power to add personal information under Clause 17(1) (12). CLPC contended that proof of identity documents dealt with in that sub-clause are personal information. The witness suggested that perhaps the secretary does not have the power under the bill to add 'new classes (in original) of personal information to the Register'.<sup>62</sup>

3.116 Such contentious issues aside, there remain many areas of discretion in the bill where no Parliamentary oversight or external review is provided.

3.117 The Victorian Privacy Commissioner observed, for example, that Clause 16 gives the secretary wide discretion to determine the form and manner in which the

---

58 Liberty Victoria, *Submission 35*, p. 13.

59 Cyberspace Law and Policy Centre, *Submission 43*, p. (2).

60 Liberty Victoria, *Submission 35*, p. 1.

61 Australian Government, *Submission 39*, p. 82.

62 Cyberspace Law and Policy Centre, *Submission 43a*, p. (2).

Register is kept. The Commissioner recommended that because these matters will have a significant impact on the privacy interests of individuals they should be set out in the legislation or regulations.<sup>63</sup>

3.118 The Australian Government Office of the Privacy Commissioner informed the Committee that the following determinations should be subject to additional oversight mechanisms, independent review, clear Ministerial direction or specific criteria, including determining:

- (a) what proof of identity (POI) information and documents are needed for registration (s 13(2));
- (b) the form or manner in which the register may be kept;
- (c) what information about an individual's benefit cards will be held on the register and the chip (respectively – s 17, item 7; and s 34, item 10); what proof of identity (POI) information and documents are needed for registration (s 13(2));
- (d) what proof of identity documents (or information about those documents) will need to be scanned and placed on the register (s 17, item 12); and
- (e) when applying for an access card, what 'other specified information' or documents that the secretary deems necessary: (i) to be satisfied of the applicant's identity, or (ii) to obtain information required for the card or the register (s 23(2)(b))

3.119 The Office suggested that items a), d) and e) in particular should be subject to parliamentary scrutiny.

3.120 The Office also suggested that the bill could usefully promote community confidence by including a general provision that these powers be exercised in consultation with the Privacy Commissioner. It considered that section 212(2)(a)(vi) of the recently enacted Anti-Money Laundering and Counter-Terrorism Financing Act 2006 provides a possible example of such a provision.<sup>64 65</sup>

---

63 Office of the Victorian Privacy Commissioner, *Submission 48*, pp 8-9.

64 Office of the Privacy Commissioner, *Submission 46*, pp 7-8.

65 The relevant section of the Anti-Money Laundering and Counter-Terrorism Financing Act provides that in performing the AUSTRAC CEO's functions, the AUSTRAC CEO must consult with a number of officers including the Privacy Commissioner and take into account any comments made in the course of those consultations.

### ***Retention of proof of identity documents***

3.121 A number of witnesses were particularly concerned by one discretion provided for in the bill. This discretion enables the secretary to make determinations about the retention of proof of identity (POI) documents (subclause 17(2)).

3.122 Subclause 17(2) provides that Item 12 is not a legislative instrument and therefore not subject to Parliamentary oversight.

3.123 The Privacy Commissioner stated that:

A general principle of privacy law is that you collect information for a particular purpose and, once that purpose is no longer required, you delete your information unless there is a reason to keep it. We would suggest that, once verification has occurred, there should be no need to actually keep those scanned documents.<sup>66</sup>

3.124 Ms Carol Berry from the Public Interest Advocacy Centre pointed to the risks of storing POI data. She said that:

The bill also has other core problems. Copies of identity documents may be kept alongside identity information on the register, for example. The bill specifies that under clause 17, item 12, copies of documents used to prove identity may also be kept in the register. PIAC is concerned by the lack of justification for keeping copies of documents beyond their use for the purpose of verifying identity and the lack of clarity under [which] circumstances this may occur. We believe that this is an inherent risk in relation to the possibility of identity theft.<sup>67</sup>

3.125 The Fels' Taskforce in its first report advanced strong arguments against the retention of copies of proof of identity documents in the system and recommended that POI documents should not be scanned, copied or kept on file once those POI documents have been verified.<sup>68</sup>

3.126 The government agreed to try to implement the recommendation.<sup>69</sup> The department submitted that:

Consistent with the Australian Government response to Recommendation 20 in Report 1 of the Consumer and Privacy Taskforce, we are exploring relevant legislation (including the Archives Act) and business process with a view to establishing processes so that POI documents or copies of them

---

66 Ms Curtis, *Committee Hansard*, 6 March 2007, p. 40. See also Professor Greenleaf, *Committee Hansard*, 2 March 2007, p. 33.

67 *Committee Hansard*, 2 March 2007, p. 26.

68 *Access Card: Consumer and Privacy Taskforce, Report Number One*, September 2006, pp 45-49.

69 *Australian Government's Response to the Access Card Consumer and Privacy Taskforce's Advice to the Minister for Human services: Report Number 1*, November 2006, p. 10.

---

are not kept once they are no longer required for verification or fraud purposes.<sup>70</sup>

3.127 In response to a question on notice asked by a member of the Committee, the National Archives of Australia (NAA) submitted documentation that DHS had consulted NAA about the disposal of records accumulated or created by the registration authority. The Committee has noted an observation made by NAA to the effect that it is possible for the enabling legislation to make provision for the control and ultimate disposal of documents without conflict with the Archives Act.<sup>71</sup>

3.128 The Committee would expect that this will be one of the options that the department will consider when trying to give effect to the Fels' Taskforce recommendation.

3.129 Of more immediate interest is the current provision in item 17(1)(12) that the secretary may make determinations to include POI documentation in the register.

3.130 The department submitted that the secretary may make determinations to add 'technical or administrative information' to the register. Retention of proof of identity documents under 17(1)(12) apparently is considered to be an addition of 'technical and administrative information'.

3.131 The department considered the Fels' Taskforce recommendation to include 'technical and administrative information' in a legislative instrument but declined to accept the recommendation. The department argued its decision was based on the ground that much of the information relates to security matters and that 'Releasing the details of such information would provide a blueprint for hacking into the system'.<sup>72</sup>

3.132 The Committee has difficulty understanding how retained copies of proof of identity documents may, on the one hand, be defined as 'technical or administrative information' and yet, on the other, how the making of a secretary's determination relating to the retention of these documents would provide a 'blueprint for hacking into the system'.

3.133 The Committee considers that determinations made under item 17(1)(12) should be disallowable legislative instruments. The Committee is also of the view that proof of identity documents should be destroyed as soon as a person's identity is verified.

---

70 *Submission 39*, p. 71.

71 *Answers to Questions on Notice, Questions from Senator Lundy 5 March 2007*, (received 12 March 2007), Question 3.

72 *Submission 39*, p. 31.

## *Delegations*

3.134 The delegation of functions under the bill was a matter of great concern to some witnesses. The delegation provisions were also raised by the Senate Committee on the Scrutiny of Bills.

3.135 That committee, in *Alert Digest 2/07*, commented on the provisions of Subclauses 68(1), 70(1) and 71(1) that permit the minister and the secretaries of human services and veterans' affairs to delegate many of their powers and authorities to a wide group of persons. The committee noted that there was little explanation of these wide discretions in the Explanatory Memorandum and sought the minister's advice:

as to whether the various subclauses relating to delegation of power might impose some limit on the type or nature of the powers and functions which may be delegated in any particular instance, along the lines of the limitation in proposed new subsection 95A-11(2) of the Aged Care Act 1997, which requires the Aged Care Commissioner, in exercising his or her powers to delegate, to 'have regard to the function to be performed by the delegate and the responsibilities of the APS employee to whom the function is delegated'.<sup>73</sup>

3.136 The Scrutiny Committee drew senators' attention to those provisions 'as they may be considered to make rights, liberties or obligations unduly dependent upon insufficiently defined administrative powers ...'<sup>74</sup>

3.137 The Australian Government submitted that the delegation provisions in the bill are consistent with the usual delegation provisions in Commonwealth legislation,<sup>75</sup> but that the Office of the Access Card was currently undertaking consultations before finalising the policy with respect to delegations.<sup>76</sup>

3.138 It is not clear to the Committee what the latter statement means. Is the Government reconsidering the provisions relating to delegations or is it merely consulting on how the provisions are to be effected?

3.139 The Committee would expect in the light of community concerns and particularly the concerns of the Senate Scrutiny of Bills Committee that the Government will revisit the whole matter of the delegations provided for in the bill.

---

73 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No. 2 of 2007*, 28 February 2007, p. 28.

74 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No. 2 of 2007*, 28 February 2007, p. 28.

75 Australian Government, *Submission 39*, p. 65.

76 Australian Government, *Submission 39*, p. 66.

---

## Conclusions

3.140 The Committee has concluded that public and parliamentary confidence in the Access Card would be enhanced if more legislative provision were made for Parliamentary and other external review (such as the Senate Standing Committee on Regulations and Ordinances), especially of the bill's more contentious elements. The suggestions made by the Privacy Commissioner in that regard about this bill would be of particular value. This would require that the bill be amended appropriately.

3.141 The wide-ranging delegations provided for in the bill are also an issue that should be addressed by the Government in this legislation, particularly in the light of the Scrutiny of Bills Committee's concerns.

3.142 The Committee understands that at least some of the matters relating to the discretions provided for in the bill have been considered in the Consumer and Privacy Taskforce's discussion paper on registration that has only very recently been provided to the minister.<sup>77</sup>

**3.143 The Committee considers that the government should take the following matter into consideration when drafting the consolidated bill:**

**Whether the following determinations should be made by way of legislation or disallowable legislative instrument:**

- (i) what proof of identity (POI) information and documents are needed for registration (clause 13(2));**
- (ii) what proof of identity documents (or information about those documents) will need to be scanned and placed on the register (clause 17, item 12); and**
- (iii) when applying for an access card, what 'other specified information' or documents that the secretary deems necessary: (i) to be satisfied of the applicant's identity, or (ii) to obtain information required for the card or the register (clause 23(2)(b)).**

## Administrative review

3.144 There are no provisions in the bill for the administrative review of decisions.

3.145 This matter was raised in the Scrutiny of Bills Committee's Alert Digest referred to earlier in this section of the report. The committee drew senators' attention to the fact that the absence of appeal rights in the bill might make rights, liberties or obligations unduly dependent on non-reviewable decisions.

---

<sup>77</sup> The Explanatory Memorandum (p. 63) states that there is merit in treating privacy issues in a holistic manner and addressing some of these protections in the access card legislation and that this is an issue that will be fully considered in the development of the second tranche of legislation.

3.146 The Government has stated in the Explanatory Memorandum that the bill does not provide any express administrative review mechanisms and that these mechanisms will be included (together with several other matters, including privacy issues and governance) 'in the second tranche of legislation'.

3.147 The Government has given an undertaking that:

Appeal rights will not be diminished and will be consistent with those in place for existing cards and entitlements. The form of that review mechanism will be the subject of advice from the Taskforce.<sup>78</sup>

3.148 The Scrutiny of Bills Committee has sought the minister's advice as to whether appeal rights could be included in this bill, together with the decision-making powers.<sup>79</sup>

### **Conclusions**

3.149 No doubt the minister will respond promptly to the concerns of the Scrutiny of Bills committee. In framing those provisions the Government should be mindful that this is an issue of great concern to many in the community.

### **Access**

3.150 Many witnesses were concerned about the matter of who would have access to the Register and to the card.

3.151 The Public Interest Advocacy Centre (PIAC), for example, submitted that it is unclear who would have access to the database that is being created as a core part of the scheme.<sup>80</sup> The Victorian Privacy Commissioner stated that the bill is silent as to who will be able to access or use information on the Register, and for what purpose.<sup>81</sup>

3.152 Both witnesses considered that the question of access should be explicit in the legislation. PIAC proposed that the issue of access should be addressed in the principal legislation rather than in subordinate regulations.<sup>82</sup> The Victorian Privacy Commissioner recommended that the bill should address who has access to the information on the Register, and for what purpose and stated that, 'The Bill should not be passed without addressing this issue'.<sup>83</sup>

---

78 The Parliament of the Commonwealth of Australia, House of Representatives, *Human Services (Enhanced Service Delivery) Bill 2007; Explanatory Memorandum*, Circulated by the authority of Senator the Hon. Ian Campbell, Minister for Human Services, p. 63.

79 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No. 2 of 2007*, 28 February 2007, p. 29.

80 Public Interest Advocacy Centre, *Submission 44*, p. 3.

81 Office of the Victorian Privacy Commissioner, *Submission 48*, p. 9.

82 Public Interest Advocacy Centre, *Submission 44*, p. 3.

83 Office of the Victorian Privacy Commissioner, *Submission 48*, p. 9.

3.153 The Government stated that:

Only authorised people will be permitted access to your information and they will have access only to those fields of information that they need to deliver health benefits and veterans' social services to you. Transactions involving the card will be securely logged, including access, authentication and the specific details of the transaction. All logs will be analysed constantly for anomalous behaviour.<sup>84</sup>

3.154 The Government informed the Committee that it had been suggested in some submissions to the exposure draft of the bill that the definition of 'authorised persons' needed clarification and that the category of Commonwealth officers who could be authorised was too broad. The Government had responded to those concerns by providing that Commonwealth officers from non-participating agencies must be in an agency listed in the regulations.<sup>85</sup>

### *Authorised persons*

3.155 The term 'authorised person' is defined in Clause 72. That clause provides that the Secretary may, in writing, appoint:

- (a) a Commonwealth officer in a participating agency; or
- (b) a Commonwealth officer prescribed by the regulations; or
- (c) an individual prescribed by regulations;

to be an authorised person for the purposes of a specified provision of this Act in which the expression 'authorised officer' occurs

3.156 The 'participating agencies' are specified in Clause 5 and are;

- The Department of Human Services
- The Department of Veterans Affairs
- The Chief Executive Officer of Medicare Australia
- The Chief Executive Officer of Centrelink
- Australian Hearing Services
- Health Services Australia Limited

### *Participating agencies*

3.157 If the Access Card is to meet its objective of improving access to Government benefits, it is obviously necessary that employees of the participating agencies must have access. There are concerns, however, that other agencies, especially those with

---

84 Australian Government, *Submission 39*, pp 81-82.

85 Australian Government, *Submission 39*, pp 79-80.

investigative functions, such as the Australian Taxation Office, may have access to the Register.

3.158 It is clear from Clause 72 that this would require that a disallowable regulation be tabled in the Parliament. However, an amendment to the legislation to appoint additional participating agencies would be a much more transparent and positive process.

### ***Conclusions***

3.159 The Committee would prefer that all proposals to add additional participating agencies and to appoint other organisations and individuals as authorised persons should be by way of legislation, rather than by regulation. It considers that the current provision to make appointments by way of disallowable regulations in most cases may represent a reasonable compromise between the need for parliamentary accountability and the administrative and legislative load that could be involved if all appointments were to be made by legislation.

3.160 Nevertheless, given the apparent high levels of community concern and the fact that the access card is not an identity card, proposals to appoint any additional participating agencies should be made by way of legislation.

3.161 An interesting issue that arose during the inquiry was the desire of the Australian Federal Police (AFP) to have investigating officers exempted from the offence provision in Clause 57 that prohibits unauthorised persons from copying the information or imaging the card.<sup>86</sup> If the AFP were to be given a specific exemption or if the AFP were to be appointed a participating agency, that should be done by way of legislation.

**3.162 The Committee considers that the government should take the following matter into consideration when drafting the consolidated bill:**

**Whether any proposals to appoint additional participating agencies should be made through legislative amendment of the principal act.**

### ***Access to information on the chip***

3.163 DHS informed the Committee that access to information on the Commonwealth's areas of the chip will be as follows:

- (a) approved Department of Human Services (DHS) and Department of Veterans' Affairs (DVA) officers and officers of agents issuing the access card. DHS and DVA will use secure terminals operated in a secure environment by approved officers.
- (b) Pharmacists and general practitioners will use secure terminals to access limited information. That information is expected to be limited to the

---

86 See *Committee Hansard*, 6 March 2007, p. 6ff.

person's name, concession status and Medicare number. Software controlling the card readers will be used to customise and limit the information which can be seen on a need to know basis.

- (c) Third party concession providers will use readers that will only reveal concessional status.<sup>87</sup>

3.164 It has not yet been decided what information will be included in the consumer area of the chip. Nor has a decision been made about how any such information may be viewed or updated. According to DHS:

Procedures for viewing and updating of information in the consumer area of the chip are the subject of separate consultations being conducted by the Consumer and Privacy Taskforce.<sup>88</sup>

3.165 This once again highlights the inadequacy of the piecemeal nature of the legislative process of this bill.

### ***Law enforcement and national security agencies***

3.166 The question of access for law enforcement and security agencies was pursued during the inquiry.

3.167 The AFP currently has access to DHS databases and other information held by Commonwealth agencies under certain legislative conditions and under certain defined conditions may not require a warrant to access that information. The Australian Security Intelligence Organisation (ASIO) may also gain access to the current databases without a warrant, but apparently may do so only at the discretion of the secretary. In a supplementary submission, DHS confirmed oral evidence given at previous Senate committee hearings that:

... ASIO may ask DHS for information from the access card Register. DHS has the discretion to give or not give that information to ASIO. If DHS does not give that information to ASIO, ASIO can only compel DHS to give that information to it in accordance with a search warrant issued pursuant to the ASIO Act 1979.

The Director-General of Security has already outlined ... the significant safeguards and accountability mechanisms to which ASIO is subject.<sup>89</sup>

3.168 Ms Scott, Secretary of the Department of Human Services, informed the Committee that in the past two and a half years she had only on one occasion refused

---

87 Department of Human Services, *Answers to Questions on Notice, Questions from Senator Stott-Despoja*, 27 February 2007, (received 9 March 2007), Question 11, p. 11.

88 Department of Human Services, *Answers to Questions on Notice, Questions from Senator Stott-Despoja*, 27 February 2007, (received 9 March 2007), Question 11, p. 11.

89 Department of Human Services, *Submission 39a*, p. 21.

a request from a law enforcement agency for access to information, apparently because the request was not sufficiently defined.<sup>90</sup>

3.169 Professor Fels suggested that AFP and ASIO access to the register should be set up in the access card legislation if possible, rather than relying on other acts.

### ***Conclusion***

3.170 The Committee considers that access to a single database covering the great majority of the Australian population, complete with biometric data, would no doubt greatly facilitate the work of the law enforcement and security agencies. Whether this would necessarily be compatible with the government's stated objectives for this legislation is another question.

3.171 The Committee has also concluded that the Secretary of the Department of Human Services should report on the exercise of discretion in relation to the access requests made by the law enforcement and security agencies. This could perhaps be done in the department's annual report in such a way as not to compromise any operational matters or matters of national security.

3.172 The Committee saw value in the Professor Fel's suggestion that access for the law-enforcement and security agencies should be set out in the access card legislation, rather than in other acts.

**3.173 The Committee considers that the government should take the following matters into consideration when drafting the consolidated bill:**

**Whether access of law enforcement and security agencies to the information in the register should be specified in the access card legislation; and**

**Whether any exercise of discretion by the secretary of DHS to grant law enforcement or security agencies access to the register should be reported to the Parliament, perhaps in the agency's annual report in such a way as not to compromise operational matters or national security.**

### ***Individuals prescribed by regulations***

3.174 Providers of services such as medical practitioners will require access to sufficient information on the card to enable them to provide a service for which people may claim a Government benefit. Presumably the secretary will seek to appoint medical practitioners and pharmacists as a class of 'authorised persons'.

3.175 The Committee understands that these individuals would have access only to those features on the card that would be required to perform a service, such as a GP

---

90 Ms Scott, *Committee Hansard*, 6 March 2007, p. 95.

consultation, and that the system would employ a range of technological protections.<sup>91</sup> Given that DHS expects that there will be 50,000 terminals,<sup>92</sup> the scheme's success will rely heavily on the choice and application of robust and appropriate technology to ensure that these protections are delivered.

## Offences

3.176 In the little time that the Committee had to consider this bill, it was not possible to cover all the issues raised in the evidence concerning the penalties that would be imposed by this legislation. The following comments relate mainly to the penalties imposed by Part 4, Division 2 – Offences for requiring production of an access card, and to an issue relating to Clause 57 – Unauthorised copying.

### *Clauses 45 and 46*

3.177 According to the Explanatory Memorandum a major objective of the Government's policy is that access cards are not to be used as national identity cards and for that reason, Clause 45 makes it an offence for persons intentionally to require a card holder to produce the card for identification purposes. Clause 46 prohibits persons from intentionally requiring a card holder to produce his or her card as a pre-condition to the supply of goods or services.<sup>93</sup>

3.178 A matter of concern to some witnesses was that these provisions could be breached through ignorance because many people are accustomed to demanding proof of identity, for example, to verify that certain people are entitled to concessions. It was suggested that this could lead to so many breaches of the offences provisions as to bring the entire Act into disrepute. Another issue that concerned some witnesses is that it might be difficult to bring successful prosecutions under these provisions.<sup>94</sup>

3.179 The privacy guarantees included in the bill are well intentioned, but the Committee is of the view that there are serious questions about their efficacy in practice. In fact, some of these provisions could, in fact, militate towards the repeal of the very privacy provisions that they are intended to protect.

3.180 The Committee is concerned about the possibility that clauses 45 and 46 could become dead letter law because they impose draconian penalties on behaviour that is both rational and morally harmless. These provisions of the bill will criminalise behaviour that is an almost inevitable consequence of this same legislation. It is logically questionable for the government to create a document that can serve perfectly as a high quality identity document, and then to penalise those in the private sector who would want to use it for precisely that purpose.

---

91 Department of Human Services, *Submission 39a*, p. 8.

92 Ms Johnson, *Committee Hansard*, 6 March 2007, p. 111.

93 *Human Services (Enhanced Service Delivery) Bill 2007: Explanatory Memorandum*, pp 43, 45.

94 Liberty Victoria, *Committee Hansard*, 5 March 2007, pp 62-63.

3.181 It will be entirely logical for persons whose job entails requiring proof of identity to prefer the most authoritative and high quality document possible. So from nightclub bouncer to airline check-in clerk, the temptation to ask for the access card as a form of ID will only be exceeded by the willingness of individual Australian citizens to produce that same document in the face of such a request. The government provides no compelling explanation for the argument that requiring a drivers' licence as proof of identity should be legitimate, while requiring an access card as proof of identity should be punishable by 5 years imprisonment.

3.182 The Committee is concerned about the likelihood that this provision will become widely ignored in practice. This prediction is supported by evidence from NSW, where it is illegal to require a state drivers' licence as proof of identity.<sup>95</sup> This law has routinely been ignored throughout NSW since its enactment with only three charges having been brought from 1993 to 2005.<sup>96</sup>

3.183 Thus it is easy to envisage the following scenario: after almost universal registration for the access card, clauses 45 and 46 will be demonstrated to be both ineffective and excessively punitive. There will be widespread pressure on the government from a business community that is highly dependent upon reliable identification documents to repeal the dead letter, draconian prohibition against requiring the access card for that purpose. In fact, even before the bill has been enacted into law, the Australian Bankers Association argued for the deletion of clauses 45 and 46 during testimony at the Committee's hearings in Melbourne.<sup>97</sup> Some would argue that the removal of these clauses would eliminate the final obstacle to the access card becoming a *de facto* national identification card.

3.184 The Government has responded that when the card is introduced there will be a publicity or education campaign that will inform people of these provisions.<sup>98</sup> On the second issue identified above, Dr Karl Alderson, an Assistant Secretary in the Attorney-General's Department, stated that some Commonwealth criminal offences are never or rarely prosecuted but still perform a very important role, for the following reasons:

Firstly, they act as a clear statement of what people's rights and obligations are so that it is clearly set out and people know where they stand and know what they must do.

---

95 *Road Transport (General) Act 2005*, Section 175. (Formerly Section 23(1) of the *Road Transport (General) Act 1999*[Repealed] and Section 11AD(1) of the *Traffic Act 1909* [Repealed].)

96 NSW Bureau of Crime Statistics and Research, *NSW Local Court Statistics 1993 to 2005: Number of charges brought in Local Court appearances finalised*.

97 Australian Bankers Association Inc., *Committee Hansard*, 5 March 2007, pp 53ff.

98 Ms Scott, *Committee Hansard*, 2 March 2007, p. 4.

---

Secondly, for those tempted not to comply, the severe criminal penalties are designed to act as a deterrent so that people are conscious of how serious the consequences of a breach would be.<sup>99</sup>

3.185 Dr Alderson asserted that the offences provisions in the bill had been drafted to make it possible to effectively prosecute.<sup>100</sup>

### ***Clause 57***

3.186 The Australian Federal Police (AFP) informed the Committee that the AFP is concerned about the offence provision in clause 57, which would make it an offence for an unauthorised person to copy or record information from the card. It was claimed that without the ability of law enforcement officers to copy information or image the card itself, intelligence analysis and investigative activity could be significantly impeded.

3.187 It is the AFP's position that law enforcement staff need to be specifically excluded from this offence provision when carrying out law enforcement functions.

### ***Conclusions***

3.188 The Committee understands that many of the offence provisions in the bill have been inserted in an attempt to ensure that the access card does not become a national identity card. Whether these provisions will have that effect cannot now be known, but much of the evidence suggested that the card will be widely used by people to establish their identity.

3.189 The Committee considers that the provisions of Clauses 45 and 46 are consistent with the bill's stated object that access cards are not to be used as, and do not become, national identity cards, and they are not objectionable. However, the Committee considers that in all probability these provisions will be ignored in practice and will become dead letter law. If so, they will not operate as the Government intends and will not be an obstacle to the access card becoming a national identity card.

3.190 As regards the request that AFP investigators should be exempt from the provisions of Section 57, the Committee notes that the bill does not provide for this. If the Government were minded to meet the request, the Committee repeats its earlier conclusion that this should be done by way of legislation.

### **Issues not considered**

3.191 The Committee has listed below a number of issues of concern to which, due to time constraints, it has been unable to give adequate consideration:

---

99 Dr Alderson, *Committee Hansard*, 6 March 2007, pp 31-32.

100 Dr Alderson, *Committee Hansard*, 6 March 2007, pp 32.

- Whether the Privacy Act provides adequate protection in relation to the proposed access card system;
- Tensions between this bill and other Commonwealth legislation, particularly the new anti-money laundering legislation;
- Tensions between this bill and state and territory legislation and benefits regimes;
- The adequacy of fraud estimates;
- Function creep in relation to State and Territory benefits and commercial or financial uses of the card;
- Implications of the access card regime for young people and youth services;
- Technical issues, particularly the extent to which necessary technology is available in Australia, the interaction of different agency datasets and ownership and management of the new dataset if this is contracted out as proposed;
- Implications for specific groups in society, particularly people who are blind or vision-impaired, indigenous people and women; and
- More detailed information on the proposed offences and penalties associated with the access card proposal, particularly the disproportionate nature of proposed penalties compared with current penalties for similar offences.

## **Conclusion**

3.192 In the little time the Committee has had to consider the bill, a number of matters of concern have arisen. Furthermore, important measures that need to be taken into account including protections, appeals and review mechanisms are to be considered in a second tranche of legislation. The Committee has concluded that it is not possible to assess the proposed access card system in the absence of these safeguards and other measures. The Committee considers that the bill needs to be combined with the second tranche of legislation into a consolidated bill to allow proper consideration of the access card proposal.

## **Recommendation 1**

**3.193 The Committee recommends that the bill be combined with the proposed second tranche of legislation for the access card system into a consolidated bill.**

### *Matters to be taken into account*

3.194 In the process of drafting a consolidated bill for the access card system, the Committee would expect the following matters to be considered:

- 
- Whether the government should consider providing appropriate terminals or readers to those agencies and providers providing benefits and services to access card holders.
  - Whether the only mandatory information displayed on the surface of the card should be the card holder's name and that other information should be at the discretion of the card holder.
  - Whether the Commonwealth area of the chip should store existing agency identifiers and that these numbers should be used when linking a card to a participating agency database, rather than the access card number.
  - Whether the form and manner in which the register is to be kept should be set out in legislation and prohibitions such as keeping the register separate from other data bases should be expressly stated.
  - Whether the following determinations should be made by way of legislation or disallowable legislative instrument:
    - what proof of identity (POI) information and documents are needed for registration (clause 13(2));
    - what proof of identity documents (or information about those documents) will need to be scanned and placed on the register (clause 17, item 12); and
    - when applying for an access card, what 'other specified information' or documents that the secretary deems necessary: (i) to be satisfied of the applicant's identity, or (ii) to obtain information required for the card or the register (clause 23(2)(b)).
  - Whether any proposals to appoint additional participating agencies should be made through legislative amendment of the principal act.
  - Whether access of law enforcement and security agencies to the information in the register should be specified in the access card legislation.
  - Whether any exercise of discretion by the secretary of DHS to grant law enforcement or security agencies access to the register should be reported to the Parliament, perhaps in the agency's annual report in such a way as not to compromise operational matters or national security.

3.195 The matters to be taken into account listed above will be reassessed in the event of the Committee's examination of a consolidated bill.

**Senator Brett Mason**  
**Chair**



# **ALP SENATORS' ADDITIONAL COMMENTS**

## **Introduction**

The ALP Senators on the Committee agree substantially with the content of the Committee Report and the recommendation to defer the bill.

The report covers many of the important issues raised in the public hearings and submissions. It broadly reflects the concerns ALP Senators have with the legislation particularly the lack of clarity and certainty in key provisions of the bill, the impacts on privacy, the potential for the access card to become an identity card due to the presence of the photo and signature on the surface of the card, concerns with security of the information stored on the chip and database, the lack of Parliamentary scrutiny or oversight mechanisms and the inherent weakness in the offences and penalties provisions.

The ALP Senators support the Committee report's recommendation and list of matters to be taken into account, insofar as they seek to improve the access card legislation. However, there remain many unresolved issues and concerns which must be addressed before the access card system, including registration, is introduced. To resolve some of these issues, ALP Senators believe that the matters to be taken account listed in the Committee report should be more than just 'considered', as the report suggests. Most of these matters should be adopted and included in any redrafted legislation and the framework for the access card system.

## **Conduct of the Inquiry**

The Human Services (Enhanced Service Delivery) Bill 2007 is a significant and complex legislative proposal.

The first available date, having regard to the Senate sitting timetable, that public hearings could take place was Friday 2 March. The Committee has therefore had less than two weeks to consider the many written submissions, the substantial evidence given at three public hearings, the serious issues and concerns raised in respect to the bill and its implementation, and to draft and present its report.

The ALP Senators are aware that the truncated timetable for the inquiry has placed unreasonable demands both on the Chair in producing a draft report and on the Secretariat staff who have had to work excessive hours under severe time pressures.

In turn, the ALP Senators only received the final Chair's draft report late on Wednesday 14 March, the day before the final report was due to be tabled.

We agree with the concerns raised in the report regarding the lack of time to consider all issues. We also note two other issues which support deferring consideration of this legislation by the Parliament.

Firstly, the Government has stated that this is only the first part of a legislative package and that further legislation will be introduced at an unspecified date to '...deal with the review and appeal processes for administrative decisions, further elements of information protection and legislative issues relating to the use of the card, including in relation to dependents'.<sup>1</sup>

Secondly, Professor Allan Fels, chair of the Access Card Consumer and Privacy Taskforce, has yet to present a number of key reports on the implementation aspects of the access card, while the taskforce's second report on registration is with the minister but has not been released.

**ALP Senators therefore strongly endorse Committee recommendation 1 that this bill be combined with the proposed second tranche of legislation for the access card system into a consolidated bill.**

The arrogance of the Government's position is also reflected in the comments by the former Minister in the Second Reading Speech who labelled persons opposing or expressing serious concerns about the measures in the Bill as 'friends of fraud'.<sup>2</sup>

This is a despicable attack upon many reputable organisations and persons. For instance, organisations such as the Office of the Privacy Commissioner, the Australian Medical Association, Carers Australia, the Federation of Ethnic Communities Council of Australia, the Australian Banker's Association, Liberty Victoria, the Royal Australian College of General Practitioners, Legacy, MedicAlert and Vision Australia appeared during the public hearings and raised significant concerns with the legislation.

Professor Fels also expressed reservations regarding the inclusion of the biometric photo and digitised signature on the face of the card.<sup>3</sup> Many others provided considered written submissions and cogent views.<sup>4</sup>

It seems that the Government is intent on bludgeoning this legislation through and maligning its critics, rather than allowing a proper debate on the merits and detail of the access card legislation.

---

1 Human Services (Enhanced Service Delivery) Bill 2007, *Second Reading*, p. 1.

2 Human Services (Enhanced Service Delivery) Bill 2007, *Second Reading*, p. 5.

3 Professor Fels, *Committee Hansard*, pp 56-60.

4 For example, see New South Wales Council for Civil Liberties, *Submission 29*, p. 3; Australian Privacy Foundation, *Submission 30*, p. 4.

---

## Registration and the Document Verification Service (DVS)

In evidence to the Committee the Department of Human Services stated that, on average, it expects 35,000 Australians to register each day for the card over a two year period.<sup>5</sup>

This is an average but the reality is that on any day the figure could be much higher, particularly in late 2009 and 2010 when many people may realise that they will lose access to Medicare and family tax benefits unless they have applied for the access card.

ALP Senators are highly sceptical of the ability of the department and agencies to deal with this influx of applicants. We question whether there will be enough public servants trained to conduct rigorous registrations at all the locations that applicants will present to each day during the registration period.

Further, we are particularly concerned that the proposed on-line Document Verification Service (DVS) which will link the Department of Human Services to the Births, Deaths and Marriages offices in each state and territory will not be available until 2010. We are concerned that a registration process that commences in advance of the DVS being operational will be corrupted by existing problems around document authentication and proof of identity. The risk of fraudulent cards being issued in the absence of the DVS will be high. For example, a project conducted by Westpac and the NSW Registry of Births, Deaths and Marriages in 2001 found that 13 percent of birth certificates presented to banks are false.<sup>6</sup>

In estimates evidence given to the Senate Legal and Constitutional Affairs Committee in February 2007, it was confirmed that there is no intergovernmental agreement yet on what documents are sufficiently reliable for proof of identity processes.<sup>7</sup> The absence of a common agreed view on document reliability puts the registration process at further risk of subversion. It is essential for the integrity of the access card in general and the goal of combating identity theft in particular that the DVS is fully operational before access card registration commences.

### Recommendation

**ALP Senators recommend that the registration process for the access card not commence until the Document Verification Service is fully operational.**

---

5 Ms Scott, Secretary, *Committee Hansard*, FPA Committee, Additional Budget Estimates, 16 February 2007, p. 14.

6 Attorney-General's Department, *Scoping Identity Fraud*, September 2001, p. 3.

7 Mr Jordana, *Committee Hansard*, Additional Budget Estimates, 13 February 2007, pp 60-01.

## **Identity Card or Access Card?**

ALP Senators support the aims behind the access card, namely to improve the delivery of benefits and services, make it easier to deal with the relevant government agencies, reduce fraud and replace a range of cards, particularly the Medicare Card, with a smartcard. This legislation, however, does not achieve those aims.

In a most unusual move, the Bill states in Clause 6 (2) – Objects of this Act:

It is also an object of this Act that access cards are not to be used as, and do not become, national identity cards.

The very fact that the Government believes it is necessary to include this clause indicates that the card has the potential to become an identity card. In its current proposed form we believe that it is inevitable. This is because the card will on its face contain the person's biometric photograph, digitised signature and unique personal identifier number.

If the card is only intended to be for access to services then it is sufficient that such details only be included on the chip and not visible without a card reader.

**ALP Senators support the view that including the biometric photo, digitised signature and personal identifier number on the face of the card should be optional.**

## **The Extent of Ministerial Power**

This legislation will give enormous powers to the Minister and the Secretary of the Department to add private information to the database, expand the uses of the card and issue guidelines that will sidestep parliamentary oversight. For instance, the Secretary of the Department of Human Services will have the power to order original identity documents presented by a person registering for an access card to be scanned and stored on the register.

If, as many suspect, the access card becomes widely used as an identity card either voluntarily or otherwise, there will inevitably be calls from the private sector to seek access to the national registration database in order to verify the identity details of the cardholder. This will generate pressure to expand the purpose and use of the card. The capacity of the Minister and departmental secretary to permit any expansion without Parliamentary control needs to be curbed.

ALP Senators believe that the legislation should place limits on the discretionary powers available to the Minister and the Secretary and that those circumscribed powers should be subject to Parliamentary oversight.

---

## Recommendation

**ALP Senators recommend that the access card legislation limit the discretionary powers available to the Minister and the Secretary and that these powers are subject to Parliamentary oversight.**

## Offences

The offences provisions in the legislation are incomplete, poorly drafted and appear to reflect policy discussions that are still taking place rather than decided policy on conduct the Government wants to prohibit. This is a major weakness in the bill. The offence provisions and authorised uses are scattered across a variety of divisions in the bill with no clear structure. It is unclear, for instance, that there are adequate offences or penalties relating to officers of the Crown who may inappropriately access stored information.

It is also unclear which agencies are authorised to deal with the access card register – to view, change or add to it – or which agencies have the power to require the card to be produced.

We also note concerns raised by the Australian Bankers Association and the AFP about the effect of Clause 57 which prohibits information from the card being copied and the conflict this raises in situations where a person gives permission for the card to be copied.<sup>8</sup> While subsequent advice suggests some of these concerns may be unfounded, the uncertainty about these issues reflects the rushed approach to, and poor drafting of, this bill.

## Contracts and Tenders

The Committee heard the access card project will ultimately involve five primary contracts, or as they were described by the department 'procurement processes': systems administration, smart card manufacture, transaction delivery provider, terminals and infrastructure and the registration process. Two requests for tender have been released, that of systems administration and smart card manufacture.

ALP Senators note the department's decision to have five separate contracts as opposed to one lead contract. The department indicated it had investigated best practice contracting for this type of project. The aim is to maintain competitive tension within some of those contracts to reduce the risk of the access card system being 'captured' by external service providers.<sup>9</sup> This approach amounts to a departure from the Howard Government's previous poor methodology for outsourcing major IT projects.

---

8 Mr Bell, *Committee Hansard*, 5 March 2007, p. 53; Federal Agent Drennan, *Committee Hansard*, 6 March 2007, p. 6.

9 Ms Scott, Secretary, *Committee Hansard*, FPA Committee, Additional Budget Estimates, 16 February 2007, p. 8.

ALP Senators also note the department's stated purpose of maintaining competitive tension within some of those five contracts is to reduce the risk of the Commonwealth being 'captured' by external service providers.

Many technical details about the operation and implementation of the access card were claimed to be unavailable to the Committee because of probity issues surrounding the tender process.

This inhibited the Committee's inquiries into basic details regarding the technical operation of the access card. For example, when asked a question about whether 35,000 registrations per day was feasible and related questions, witnesses representing CSC, a company bidding for the systems integration tender, were predictably unable to answer because of the deed of confidentiality they had been required to sign to participate in the tender.<sup>10</sup>

This raises the question of why the tender for the systems integration of the access card had already been released to the market *prior* to the bill being debated in, let alone passed by, the Parliament. This is contemptuous of the Senate committee inquiry and has hampered the gathering of key evidence.

It also raises the possibility of the Commonwealth, having called for a response to tenders that may have to be modified or cancelled, being left in a compromised position, depending on the outcomes of the processes of the Parliament.

This has also meant that the Committee was unable to get details of the registration process. For example, CSC provided evidence that implied the contract was structured so the external service provider would not be liable if the registration process did not achieve the Government's claims of 35,000 per day. CSC identified the cooperation of the public as a key risk factor in achieving registrations to the levels foreshadowed by the Government.<sup>11</sup>

The Department also refused or was unable to provide detail regarding aspects of the technical operation of the access card, either on the ground that it would be in the next bill or that probity issues prevented disclosure. These issues fall into four categories:

---

10 See *Committee Hansard*, 2 March 2007, p. 60:

Senator Lundy—....What is in this contract that would make the winning contractor comply with that key performance indicator and what sanctions exist in the tender documents?

Mr Cook—You are aware that we are under confidentiality deeds with regard to this document.

Senator Lundy—I cannot ask you specific questions about the tender documentation.

Mr Cook—You can ask them but we cannot answer them.

11 Mr Cook, *Committee Hansard*, 2 March 2007, pp 60-61.

- The relationship (technical interface, including meta-data standards) between the existing multitude of databases in participating agencies and the new access card (Registration) database;
- The management, security and distribution of authorised card readers linked to terminals with registration database access;
- The detail of privacy safeguards, security, storage, access and archiving protocols of digitised personal, private ID information collected by the DHS through the registration process; and
- The technical features of the smartcard itself including PIN protected areas, eg. an individual's ability to protect the private part of the Card with a PIN separate to the PIN protecting information required to be held on the Card by the Commonwealth.

It is of great concern to ALP Senators that this critical information was unable to be provided. As a consequence, it is very difficult to assess the degree of privacy protection and technological and organisational security that will apply to both the access card and the registration database.

### **Recommendation**

**ALP Senators recommend that the Government not request any more tenders for access card related contracts until after consideration by Parliament of all access card bills.**

### **Other Issues**

Whilst there are a number of other issues of concern, noted in the Committee report, that warrant the legislation being deferred, ALP Senators wish to highlight three matters of concern which were raised during the public hearings, but which the department was unable to adequately address or refute.

Firstly, Electronic Frontiers noted that it was 'completely inappropriate' that the chip's design has not yet been decided. ALP Senators note that the operational features, including many practical privacy and security related issues, depend on the design of the chip itself. Hence it is extremely difficult to assess the veracity of the government's privacy and security claims in the absence of technical information and appropriate technical advice from experts on these matters.

Secondly, Legacy expressed a concern that there could be significant costs involved for war widows who have to obtain original documents for registration. The costs of identity verification were raised several times by witnesses.<sup>12</sup> The department was not able to provide detailed information as to how they would ensure that registration would be affordable for all Australians

---

12 Mr Riches, *Committee Hansard*, 5 March 2007, p. 38.

Thirdly, MedicAlert raised a serious concern that medical details stored on the access card register could create dangers because they can quickly become out of date or if the details are not verified by medical practitioners or authorities. MedicAlert is also concerned that its ongoing viability may also be threatened if the Government promotes the access card as an alternative to MedicAlert. MedicAlert provides an excellent service to hundreds of thousands of Australians. Its service is unique as the health information on their database has to be verified by a doctor.<sup>13</sup> The implications of the access card need to be clarified to ensure there are no adverse consequences for the MedicAlert system and organisation.

These three matters are further examples of the rushed approach to this legislation and the gaps in it. In view of these and other shortcomings, this bill should be deferred.

**Senator Michael Forshaw**  
**Deputy Chair**

**Senator Carol Brown**

**Senator Kate Lundy**

**Senator Claire Moore**

---

<sup>13</sup> Mr Bray, *Committee Hansard*, 5 March 2007, p. 41.

# THE AUSTRALIAN DEMOCRATS

## ADDITIONAL REMARKS

### Executive Summary

The Australian Democrats are not satisfied that the current proposal would lead to establishing a privacy compliant and rational scheme. A much more focused proposal needs to be brought forward with greater safeguards in relation to the quality, amount, and adequacy of information to be collected, used and disclosed in relation to the stated purposes of the legislation: fraud prevention and enhanced Commonwealth human services and benefits delivery. However, and most significantly, any new proposals need to have much more reliable safeguards against function creep over time, with strict legislation and independent control being crucial features.

The Australian Democrats have worked on national identification and privacy issues, including the Access card, for more than 20 years.<sup>1</sup> Because of strong campaigning by the Democrats the Access card of the 1980s never eventuated.

The proposed legislation was, in part, referred to a Senate inquiry after pressure from the Democrats to have this issue more closely examined.

The Inquiry by the Finance and Public Administration Senate Standing Committee on the proposed Human Services (Enhanced Service Delivery) Bill 2007 has considered this legislation, a number of public submissions and evidence from various witnesses in a very short space of time.

Running parallel to the Senate's inquiry have been various community consultations and Government tendering processes for aspects of the Card. These processes are all at varying stages. Some of these processes have commenced, others are yet to get underway.

The Access card database will be set up as a separate database from the databases of participating agencies. Although detailed customer records will continue to be held separately by the participating agencies, a subset of the information held in each department will flow through to the central Access card register. Further, if someone updates their address details with one participating agency the updated address details will be synchronised which will allow address details to flow through to each of the departments.

---

<sup>1</sup> The late Janine Haines, former Leader of the Australian Democrats, was one of a few well-known people to campaign against the Australia Card see *The Formation of the Australian Privacy Foundation* <http://privacy.org.au/About/Formation.html>

The project has three identified streams of activity:

- Stream 1 – Implement Access card infrastructure within legislation;
- Stream 2 – Define the frameworks for individual's space of the chip; and
- Stream 3 – Other matters such as the registration process, appeal rights, privacy protections.

Streams 2 and 3 are not sufficiently advanced to allow the privacy issues to be addressed. Much of the detail of Streams 2 and 3 has been left for the possibility of future legislation.

This Bill has been prepared with undue haste. I strongly agree with the Committee's Recommendation that this bill should be withdrawn.

However, to go a step further than the Chair, I recommend that this bill should be opposed outright. Bundling the issues contained in this proposal into a second piece of legislation without a few necessary qualifications should be discouraged. Firstly, that the Government not bring the complete package of legislation before Parliament until such time as Professor Fels' Consumer and Privacy Taskforce has reported on all aspects of the government's proposal. Secondly, the community should be offered an opportunity to comment on an Exposure Draft of any consolidated smartcard legislation.

This report discusses the key issues for the Australian Democrats with the proposed legislation. The first part of the report refers to the importance of having openness and transparency and the need for caution with attempts to compare Australia's proposed access card scheme with schemes which operate internationally. The main framework for analysis of the privacy and security risks in the proposal is a discussion of the five privacy rights: the right information, to the right people, for the right reason, in the right way, at the right time.

## **2. Openness, Transparency and Building Trust about the Technology**

The Democrats strongly advocate accountability and we value openness and transparency in government.

The way in which the Federal Government has chosen to roll-out the legislative and technical aspects of this scheme only reinforces concern the Democrats hold about trust, confidence, privacy and security in using smartcard technology and the Card itself.

Throughout the inquiry there have been several instances of a lack of openness and transparency on the part of the government about this proposal. Most notably the Government's:

- refusal to provide its Privacy Impact Assessment;<sup>2</sup>
- its non-release of its KPMG report in relation to the Access card proposal;<sup>3</sup>
- its non-disclosure of the breakdown of costings associated with the Card; and
- its claim of legal privilege and commercial-in confidence over several documents.

Several witnesses have been highly critical of the Department's lack of communication and engagement about smartcard processes and rationales. Some stated that the Department only contacted them once, while many did not hear much from the Department at all.

For example, Professor Graham Greenleaf commented:

Mr Battersby gave me an undertaking that the department would get back to me and tell me whether I was misinformed about any of the comparisons I was making. For some months I kept hounding Mr Battersby as to when I would get a reply. The question was eventually flicked on to the deputy secretary...<sup>4</sup>

Unless the Department of Human Services - which is the single agency which must conceptualise, develop, buy and use the smartcard technologies - is transparent and engages with the community, the public's perception of the technology will restrain the benefits that might otherwise flourish. People will remain wary (perhaps unnecessarily of the technology) until such time as the Government adequately explains that individuals' personal information and freedoms are protected.

## **Background**

Australians have previously rejected the idea of a national identification Card when they said no to the Australia Card in the 1980s.

Yet, because the access card legislation will make it compulsory to include a photograph and electronic signature on the surface of the Card, it appears obvious that this proposal is nothing more than a re-invented and re-vamped National Identification Card.

The Australia Card Bill 1986 was introduced into the Parliament in October 1986 by the then Minister for Health. The Australia Card Bill was rejected by the Senate, with the Australian Democrats and the Coalition voting against it.

In 1987, the Bill was reintroduced, without change. It was rejected once again by the Senate and became the trigger for a [double dissolution election in 1987](#).

---

<sup>2</sup> *Committee Hansard*, 2 March 2007, p52.

<sup>3</sup> *Committee Hansard*, 2 March 2007, p 12.

<sup>4</sup> See Professor Graham Greenleaf, *Committee Hansard*, 2 March 2007, p45.

Following the return of the Hawke Labor Government at the 1987 election, the Bill was introduced for a third time but was laid aside on [8 October 1987](#).

At the time, John Howard MP said this of the proposal:

As the weeks go by, the proposition will become more and more unpopular and I predict now the [Hawke] Government may well chicken out on the ID card.<sup>5</sup> (['Same old card trick'](#), David Humphries, The Sydney Morning Herald, 23 July 2005)

This legislation goes significantly beyond the proposed Australia Card in both reach and coverage despite government assurances to the contrary. In this context, Professor Graham Greenleaf's analysis of the failed Australia Card compared with the current proposal highlights deficiencies with the current scheme in relation to the taking of photographs, card storage capacity, data security, card readers and hacking. The privacy and security protections one would expect to see in a proposal of this nature simply do not feature.<sup>6</sup>

## **Need for reform**

### ***Government rationale***

The primary stated objectives of the Government's proposed Access card system, summarised by the Chair of this Report are:

- improving the delivery of Commonwealth human services and benefits and
- combating fraud, particularly in relation to identity theft.

The Democrats reject the assertion that the proposed legislation in its current form will deliver on the Government's stated objectives.

Firstly, thieves will continue to have access to a number of proof of identity documents, such as birth and marriage certificates. Accordingly there is no reason to doubt that thieves will continue to use such documents to register to receive an Access card.

---

<sup>5</sup> See [www.privacy.org.au](http://www.privacy.org.au)

<sup>6</sup> See Australia's proposed ID card: Still quacking like a duck , Professor Graham Greenleaf, Volume 23, Issue 2 , 2007 available at [www.sciencedirect.com](http://www.sciencedirect.com).

Secondly, the Government's service delivery model turns on a registration framework requiring an individual officer only spending 10 -12 minutes with a card holder applicant. In this time, an officer is expected to perform multiple tasks including interviewing, photocopying documents and verifying identities.<sup>7</sup>

Third, the estimate of the cost and cost-savings for the taxpayer in relation to identity fraud remains unclear.

Mr Jordan of KPMG estimated from Centrelink and Medicare alone the overall potential fraud and *leakage* in the system was 1.4 to \$2 billion annually.<sup>8</sup> This figure must be approached with caution. For example, it appears leakage might also relate to entitlement-based fraud and over servicing. KPMG have also not said how much identity fraud is used to perpetuate welfare fraud as opposed to the other types of identity fraud such as obtaining an identity card for the purposes of under-age drinking, tax evasion or credit-card.

However, in evidence from Ms Anna Johnston, Australian Privacy Foundation, the Committee was advised:

The Australian government, through the Minister for Justice, Chris Ellison, commissioned an independent report into assessing the scale of identity fraud in Australia in about 2003. Those of us working in identity management areas expected the figure to be \$2 billion. The report came down and said that it was about \$1 billion—or half of what people were expecting—and quite a big chunk of that, about 40 per cent, from memory, actually related to the cost of law enforcement in dealing with identity fraud.<sup>9</sup>

Federal Agent Drennan, in his evidence to the Committee, explained that the reason for why the Federal Commissioner for Police, Mick Keelty had given a range of between \$1 billion and \$4 billion was because “it is such a difficult thing to quantify.”<sup>10</sup>

---

<sup>7</sup> The evidence of Mr Jordana from the Attorney-General's department queried the 10-12 minute costing. Specifically he said the amount of time that it takes is an issue that they would have concerns about; it has not been the principal focus obviously of our engagement with them. As I understand the enrolment process that is envisaged, the amount of time that the applicant spends when they physically come to register, if that is the way in which they are going to be registered, would depend on how much information had been provided in advance. I gather there will be scope for information to be provided in advance so that some of the checking that is necessary could be done in advance. That will obviously have an impact on how long a person is in the office to go through the application process. I gather there is a relationship between those two. The time period has not really been an issue which is of interest to our department, per se. See Committee Hansard, 6 March, Canberra, p33.

<sup>8</sup> Committee Hansard, 2 March 2007, Sydney, p11.

<sup>9</sup> Committee Hansard, 2 March 2007, Sydney p25. See

<http://www.sirca.org.au/news/releases/2003/0302FraudBook.html>

<sup>10</sup> Committee Hansard, 6 March 2007, Canberra p14.

The Democrats consider that the evidence provided to the Committee highlight that the true cost of the extent of the problem is difficult to quantify.

*Views of members of the public*

An independent poll carried out by *The Age*, a leading newspaper demonstrated the lack of broad community support for this proposal. For example, the poll on 28 February 2007 indicated that only 28% of those polled supported the introduction of the proposed access card.<sup>11</sup>

*Views from around the world*

According to a survey by Privacy International, as of 1996, around 100 countries had compulsory identity cards. Nearly all common law countries do not have identity cards.<sup>12</sup>

Many of the witnesses both for and against the Card referred to smartcard systems that had been adopted in one form or another from around the world as justification for mandating their use in the delivery of social welfare services here in Australia.<sup>13</sup>

Several witnesses were asked the question as to what was happening with smartcards overseas.

The Senate Committee heard that varying forms of a smartcard were operating in hundreds of countries around the world. Examples of their use were in the health, national identification, public transportation, and telecommunication fields.

The Democrats believe that while Australia can learn from the experience of other countries there are significant discrepancies between overseas smartcards and the current proposed smart card before the Committee. The Democrats advocate a cautious approach in the area of international comparisons.

Mr Bill Bolton of Computer Sciences Australia stated in relation to the Belgium ID Card:

The European model is different in terms of what is acceptable with national identity cards and what is not. They happen to have started from one place and they are moving towards using that card because it is already there for delivery of social welfare.

The Australian situation is quite different; we are coming from a situation where we do not have a national identity card. So the government is implementing a card for a

---

<sup>11</sup> <http://www.theage.com.au/polls/form.html>

<sup>12</sup> See National Identification Cards available at [www.privacyinternational.org](http://www.privacyinternational.org)

<sup>13</sup> Committee Hansard, 6 March 2007, Canberra, p85, Committee Hansard, 2 march 2007, Sydney, p48, 52,64,69,

particular purpose related to social welfare and health care. The two are not automatically tied together; it just happened to be the way that, in one country in Europe, that was the flow.

There are several key differences in overseas smartcards and the proposal. These include:

- some identification systems are a result of post-war Europe identification system
- Some are a result of national security and terrorism threats
- some operate in Communist countries
- many are used to control borders
- many are limited in their functionality
- few are mandatory to carry and produce
- few are multifunctional and
- there are variations in the type of biometrics on the surface of the card.

While a detailed comparison of the proposed card with international cards has not been possible in the limited time available for this inquiry, it is worth noting that many ID cards from around the world have had something go wrong with them. For example:

- in Holland a citizen dressed up as the joker from Batman<sup>14</sup> and was issued with an ID card and
- in Estonia it was discovered that the sealed security envelopes containing the secret PIN and PUK codes issued with the cards were transparent when placed under an ordinary light bulb.<sup>15</sup>

### **Five rights approach to assessing the proposal**

The Democrats refer to the former New Zealand Privacy Commissioner, Bruce Slane's eloquent summary of privacy laws. Mr Slane described the privacy principles as essentially about the right information to the right people, for the right reason, in the right way at the right time.

The Democrats consider this provides an excellent framework in which to assess the card and the actual ID card system and the privacy and security aspects of the Human Services (Enhanced Service Delivery) Bill 2007.

### **The right information**

The Democrats do not believe that the Government has got the right information on the surface of the Card, in the register, or in the chip.

---

<sup>14</sup> See <http://www.dutchnews.nl/news/archives/2007/01/>

<sup>15</sup> <http://www.privacyinternational.org/survey/phr2003/countries/estonia.htm>

---

*The Card surface information*

Clause 30 of the Bill states that information displayed on the surface of the card will include:

- a photograph
- an electronic signature
- an access card number

The photograph, electronic signature and access card number should not be on the surface of the card. If they belong anywhere, then at the very least they should be on the chip, protected by strong security provisions. Putting this level of detail on the card would diminish privacy rights because:

- it will only increase the likelihood that the card will be used as a defacto national identity card<sup>16</sup>
- it is likely that in at least 50% of cases staff matching people to the photos in the card will make an incorrect match<sup>17</sup>
- individuals who steal a card will be able to more easily modify there appearance to look like the photograph on the surface of the card
- the number and signature may lead to fraud and identity theft<sup>18</sup>

*The register information*

The fields to be completed by an applicant are too expansive and are not supported. It is a well founded principle of privacy law that the minimum amount of personal information necessary to give effect to legally authorised functions and activities is the minimum amount of information an agency should collect.

There are also instances of many staff of various Commonwealth agencies inappropriately accessing personal information. The less information that is contained

---

<sup>16</sup> For example, See Privacy Victoria submission, Access card No way Submission, Australian Privacy Foundation Submission, Public Interest Advocacy Committee Submission, Graham Greenleaf submission, Liberty Victoria submission

<sup>17</sup> In an experiment at a London supermarket, more than 50 per cent of fraudulent cards were accepted. Richard Kemp, from the Department of Psychology at Westminster University, told the British Psychological Society conference in London in 1996. Matching a photo to a stranger's face was 'too difficult'. Dr Kemp's team took over a supermarket staffed by six regular cashiers who were warned to look out for fraudulent cards. A group of 44 students acted as "shoppers" armed with four photo credit cards; one with a photo as the student looked, one with cosmetic changes, and two fraudulent cards of someone who resembled the student and one of someone totally different. Overall more than half of fraudulent cards were accepted; including 64 per cent of the cards bearing a photo of someone who looked similar to the student, and 35 per cent of the other type of fraudulent cards. See [http://findarticles.com/p/articles/mi\\_qn4158/is\\_19951221/ai\\_n14025133](http://findarticles.com/p/articles/mi_qn4158/is_19951221/ai_n14025133)

<sup>18</sup> Professor Alan Fels, *Committee Hansard*, 6 March 2007, p. 63

in the register then the less attractive it will be for Commonwealth employees to snoop on citizens.<sup>19</sup>

The Democrats do not support the inclusion of the following fields on the register:

- titles such as Mr, Mrs, Ms and email addresses. These will quickly become inaccurate and will result in poor data quality.
- residential and postal addresses. Australians should have a choice as to whether they provide their home address. For some vulnerable Australians they may not wish to divulge their home address to upward of 5 different agencies<sup>20</sup>
- registration status. Temporary information passing through the Register such as a person's interim status should not be contained in the register. A person should be registered or unregistered. Temporary information breeds uncertainty, establishes a window of opportunity in which to masquerade as somebody else, and runs the risk of lending itself to discrimination against sections of the community
- storage of Proof of Identity (POI) documents after identity is established. Given the value of these documents in proving identity, and that a contributing factor in identity fraud is people using such documents to obtain real identities, copies of birth certificate, passports, marriage certificates should not be stored on the register indefinitely
- The flag if you have a relationship with a participating agency if it is to be used to label a person. Presumably the point of having a 'Centrelink' flag against a person's name is to allow Centrelink to look at a record to check a person's current address and conversely if a person is not a client of Centrelink, no flag should exist and there should be no access. However, the lack of a definition of 'relationship' may mean flags can be used subjectively to infer such things as 'difficult customer' 'manic behaviour' 'takes longer to deal with.'

---

<sup>19</sup> Centrelink, the Child Support Agency and the ATO have each recently admitted they have found multiple cases of staff inappropriately accessing, amending, using and disclosing customer records. Centrelink found 600 staff over a two-year period had committed 790 breaches. The Child Support Agency discovered 405 breaches, including 69 cases where sensitive information including addresses was given to former spouses; in two cases the Government had to pay to relocate families for their own safety. See "Centrelink staff sacked for privacy breaches", ABC News Online, 23 August 2006, [www.abc.net.au](http://www.abc.net.au); "Eyeing Big Brother", The Canberra Times, 26 August 2006; "Tax office sacks 'spies'", The Australian, 29 August 2006, p.1; "Federal blitz on snoops boosted", The Australian, 29 August 2006, p.33; and "No leaks but 27 stickybeaks inside ATO", Australian Financial Review, 30 August 2006, p.4.

<sup>20</sup> The 1989 murder in the US of actress Rebecca Schaeffer occurred because in spite of her having an unlisted telephone number and address a stalker tracked her down through the state motor vehicle records. One of the early conciliations in the office of the Victorian Privacy Commissioner included payment of compensation of \$25,000 after a government body had disclosed the complainant's new name and address to her violent ex-partner despite her having made a request to the body not to release this information to anyone. See: *Privacy Avoiding the pitfall*, Address to the Victorian Government Solicitor's Office, Helen Versey, Victorian Privacy Commissioner 26 October 2006, [www.privacy.vic.gov.au](http://www.privacy.vic.gov.au)

In relation to the issue of confidentiality of address information, further support for allowing individuals the option of suppressing this information can be found in Victoria's newly enacted Victims of Crime Charter. This Charter sets out principles on how the criminal justice system and victim support agencies should respond to victims of crime.

The Victims' Charter is contained in legislation called the Victims' Charter Act 2006 which became law on 1 November, 2006. Relevantly, if you are the victim of crime, you have the right to:

Have your personal information, including residential address and telephone number, not disclosed to anybody except in accordance with the Information Privacy Act 2000

Equally, in NSW the Coordinator of the NSW Victims of Crime register allows victims to provide a mobile telephone number to receive SMS texts or email address instead of a residential address.

The Access card requirement that the register must list a person's residential address is a grave threat to Victims of Crime programs around the country.

While there is scope in the legislation (at clause 65) for the Secretary of DHS or DVA to exempt an individuals from the requirement to have his or residential address included in the Commonwealth's area of the chip there is no guarantee to Victim of Crimes that this will happen. More importantly, an individual who makes such a request has no right to appeal any decision by a Secretary who may refuse suppression.

#### *The information in the Commonwealth area of the chip*

The Democrats strongly oppose the inclusion of the following fields on the Commonwealth's area of the chip:

- residential and postal addresses for the reasons listed above
- other technical and administrative information.

The Explanatory Memorandum states that this is intended to relate to audit logs and the serial number of the chip. The retention of log files may be privacy enhancing for auditing purposes but this is dependent on what the log files contain, how they are accessed and by whom. More detail about what is to be retained, for what purpose, for how long, and who will get access to these log files is needed.

#### *The information in the individual's area of the chip*

Senator Stott Despoja asked the Department of Human specifically about the intent of Clause 33A of the proposed legislation which refers to the individual section of the chip. She said:

---

My understanding is that the government has been emphasising that this particular piece of legislation is about the Commonwealth's responsibilities. This legislation deals with the Commonwealth area of the card. Why is there legislation now dealing with the individual section of the card?

In response to this question Ms Kathryn Johnson, of the Department of Human Services stated:

The legislation was built as a framework to indicate to people that there were going to be two parts of this chip of the card—a part that the Commonwealth owned and that the Commonwealth had protections in relation to, and parts that 'you'—that is how the legislation is written—will own and you will have access to. It was intended with the legislation just to set that framework. It was the intention that we would not otherwise deal with that area of the chip, because it is subject to the Consumer and Privacy Task Force work, which they are doing as we speak. There are no other references to that area and no other law in relation to that area, apart from frameworks indicating that it will exist.

The Democrats do not, at this stage, see merit in legislating for the individual section of the Card. We have arrived at this conclusion because:

- it lacks qualitative and quantitative evidence from the Australian community that an individual area is welcomed
- it detracts from the purpose of the Act which is to facilitate the provision of benefits services, programs or facilities under a Commonwealth law
- it lacks detail about what information should be kept in this part of the chip and what information is broadcast from this section of the chip to the card readers when swiped<sup>21</sup>
- it essentially centralises on the chip private and public interests which may not necessarily be complementary
- the more personal data we put on the card the more prone it will become to attack and function creep
- the government has not ruled out charging consumers a fee for service in relation to this part of the chip<sup>22</sup>

---

<sup>21</sup> The individual section of the chip is still subject to ongoing consideration by the government's Privacy and Consumer Taskforce which has issued a Discussion Paper No 2 titled "Voluntary and Medical information" available at [www.accesscard.gov.au](http://www.accesscard.gov.au)

<sup>22</sup> Senator Stott Despoja asked the following Question on Notice of the Department of Human Services dated 27 February 2007: Will applicants have to pay any money toward the cost of the new card, including loading information to the consumer side of the chip and obtaining a pin number? In reply the Department stated: "It remains an open question as to whether there should be some charge for this service, and if so, who should bear that charge. The general position of the Taskforce is that, since this facility is being accessed at the choice of the individual cardholder it could be the responsibility of the individual to bear the costs associated with it".

## **The right people**

Participating agencies of Centrelink, Medicare Australia, Australian Hearing Services, Health Services Australia Limited, the Department of Veterans' Affairs and the Department of Human Services (including the Child Support Agency and CRS Australia) will have access to personal information.

### *Agencies with a need to confirm concession status*

The Explanatory Memorandum in relation to Clauses 45 and 46 states:

For example, some service providers provide some of their services at discounted rates to pensioners or to persons who are entitled to particular kinds of Commonwealth concessions.

Subparagraph 46(1)(d)(i) is intended to ensure that these service providers can continue to provide these discounted rates to persons who are entitled to the relevant concession.

Accordingly, it will not be an offence for a provider to refuse to provide a service at a discounted rate if a person refuses to produce his or her card to verify that they are entitled to the relevant concession.

At the Canberra hearing Ms Patricia Scott, Secretary of the Department of Human Services confirmed an additional feature of the smartcard is that it can be used as a concession card. Specifically, she stated:

The cards that are being collapsed into this include a range of Concession cards—the Safety Net concession card, the Prescribed Patient Cleft Pallet and Cleft Pallet Scheme concession card, the Prescribed Patient card.

Data about concession status and eligibility is to be stored in the Commonwealth controlled section of the chip.

The use of the Access card as a Concession Card enables a multitude of agencies access to the Commonwealth area of the chip. Many examples of the type of agencies who would be able to access a person's concession status were presented to the Committee. These included:

- state public transport agencies<sup>23</sup>
- agencies who sell bus tickets<sup>24</sup>
- agencies who sell movie tickets<sup>25</sup>

---

<sup>23</sup> Ms Kathryn Johnson, Department of Human Services, Committee *Hansard*, 6 March 2007 p117.

<sup>24</sup> As above

<sup>25</sup> As above

- the local video shop<sup>26</sup>
- a pharmacist<sup>27</sup>

The extent of the number of agencies to who might be able to gain access to concession status and how this will work in practice is of great concern.

The evidence of Ms Irene Graham, from Electronic Frontiers Australia, on this matter was compelling. At the Melbourne hearing, Ms Graham said:

The current proposal appears to be that there will be only one personal identification number applicable to the chip, if the person chooses to have a PIN. This will apply to the Commonwealth area. The Commonwealth area will obviously be the area that also has any information about the chip in it.

There therefore appear to be two options. If you have a PIN on your chip then, when you are at the cinema and you want to prove that you are entitled to a concession, you will have to enter your PIN to open up the Commonwealth area.

Now what is going to stop all the information on the chip from being disclosed to the cinema person—as distinct from just, for example, the letter ‘C’?

The answer to this question is—and this is how smartcard technology works—that it depends on the smartcard reader that you are docking the card in. The card reader needs to have technology in it that uses various technological systems like cryptography and passwords so that effectively what happens when you put the card in the card reader is that the card says to the card reader: ‘Are you an authorised card reader? Can you prove that you have software in you that the government has provided that says, “I can tell you just this one piece of information that you want,” for example, C?’

So card readers that currently exist in Australia Post or in Dick Smith—if they even exist there or anywhere else—cannot be used in the way that the government or the DHS representatives are currently talking about because, at the very least, they are going to need special software in them to control access to the card.”

The reference to Dick Smith or Australia Post Card readers was mentioned by the Secretary at the Canberra hearing on 6 March 2007, after Ms Graham had provided her evidence. Ms Scott stated that the card readers were:

...very small, and I am sorry I do not have them with me but we have brought them along to almost every other hearing. They were used at the Atlanta Olympics and at all sort of places where, for privacy, you insert the card and the concessional status would be visible.

---

<sup>26</sup> Ms Helen Versey, *Committee Hansard*, 5 March 2007, p. 8.

<sup>27</sup> As above

Then there are the USB type readers that you can buy at Dick Smith's. That is a very simple little device with a cord into it. You whack it into your computer, you insert the card and so on. It would not read all parts of the chip. Then there is the smartcard reader that businesses will have because credit cards and debit cards are going smartcard"

### *Law enforcement agencies and ASIO*

It is important to note that lurking in the background of the government's proposed access card and register of 16.7 million Australia's are Federal and State Law enforcement agencies and the Australian Security Intelligence Organisation (ASIO) wanting to gain access to private information for criminal intelligence purposes.

Post September 11 and the Bali bombings, the scope of these agencies' law enforcement powers has significantly been broadened.<sup>28</sup>

At the hearing in Canberra, the evidence from Federal Agent Peter Drennan, Acting Deputy Commissioner, Australian Federal Police and Mr Paul O'Sullivan, Director-General, Australian Security Intelligence Organisation, confirmed the Democrats concerns that the database supporting the access card could be used for criminal intelligence purposes.

The Democrats make special mention of the following matters:

- it is debatable whether ASIO will require a warrant from the Attorney-General in order to seek information from other Commonwealth agencies participating in the Access card proposal<sup>29</sup>,
- Federal Police rely on the provisions of the Privacy Act, in that where there are legitimate reasons for other agencies to disclose that information to us then they can do so.<sup>30</sup>

The centralised database of 16.7 million Australians will be a powerful tool in the detection and investigation of crime.

There is a need to balance public sensitivities which will surround the trial and adoption of a new technology such as a smartcard, the breadth of information on the card, in the register and on the chip, and access to personal information by law enforcement agencies.

The bill currently contains no additional safeguards preventing inappropriate access by law enforcement agencies.

---

<sup>28</sup> For example, the Anti-Terrorism Act 2005 (Cth)

<sup>29</sup> Mr O'Sullivan *Committee Hansard*, 6 March, 2006 p13

<sup>30</sup> Federal Agent Peter Drennan *Committee Hansard*, 6 March, 2006 p17

The only safeguards to which the Committee referred were those which exist in the *Privacy Act* and specific law enforcement legislation such as the Australian Security Intelligence Organisation Act 1979 (Cth).

The Democrats find little comfort in the protections afforded to Australian citizens in the *Privacy Act* (incidentally at this time under review) and recommend fit-for-purpose law enforcement access arrangements be specifically spelt out in this legislation.

The Democrats are deeply dissatisfied with the Secretary's response to the line of questioning in relation to how she makes her decisions about whether or not to disclose personal information to assist law enforcement agencies. All that the Secretary could do was state that she had considered the provisions of the *Privacy Act*.<sup>31</sup>

In a follow-up Question on Notice directed to the Secretary about this issue, Senator Stott Despoja asked: Can the Department please provide a copy of their current privacy policy and written guidelines that the Secretary follows in making a decision about whether or not to disclose personal information pursuant to IPP11?

In reply the Department of Human Services stated:

We refer to the extract of Senate Inquiry Hansard on 6 March 2007 set out below:

Ms Scott—We have to deal with each case on a case-by-case basis. Certainly the Privacy Commissioner can assist. For example, in the tsunami a question arose about whether we could utilise information available in the agencies to assist in the tsunami recovery, and the Privacy Commissioner's advice was sought there. That is one source of information. I can take legal counsel, and I would on some of these matters. I did on the case that I referred to earlier. It has to be done on a case-by-case basis. It is not like there is an easy, simple set of rules. Bali was different from anything else that we had encountered.

No privacy policy nor written guidelines were provided by the Secretary. This only reinforces the potential privacy intrusiveness of the scheme without proper accountability measures and casts doubt over the Secretary's ability to exercise the many discretions granted to her under this proposal.

The Democrats will move an amendment to the legislation to include provisions setting out when and how law enforcement agencies (Commonwealth, State and Territory) and ASIO can obtain access to information and when a warrant will be necessary.

---

<sup>31</sup> Ms Scott, *Committee Hansard*, 6 March 2007, p 101

An appropriate model for warrants permitting access to information in the Access card Register would be the interception warrant, or stored communication warrant, provisions of the *Telecommunications (Interception and Access) Act 1979*.

*The Minister, Secretary, and the Secretary's delegates*

Liberty Victoria has identified 29 separate discretions that are vested in the Minister by the Bill, which include 23 discretions vested in the Secretary that are subject to Ministerial direction under Clause 8 of the Bill.<sup>32</sup>

In addition, subclauses 68(1), 70(1) and 71(1) permit the Minister and the Secretaries of Human Services and Veteran's Affairs to delegate many of their powers and authorities to a wide array of individuals who may not necessarily be senior officials.

The Democrats do not believe, in most instances, that the Minister, Secretaries and their delegates, are necessarily the right people to be determining what proof of identity information and additional documents are required in this scheme. The right body should be Parliament.

*Minority Groups*

The Democrats share the views of several witnesses that care and compassion with ethnic and other minority groups is required in order that they feel comfortable with the registration process, the information on the surface of the card, and the design of the card.

No one group should be disadvantaged under the proposed scheme. What is of essential importance is the provision of delivery of health and social service benefits. Of lesser importance, is the means in which these services are delivered.

The Committee heard evidence from representatives of different cultural communities about how ethnic communities might feel marginalised as a result of some of the features of the Access card.

Mr van Vliet of Federation of Ethnic Communities Councils of Australia highlighted the sensitivities and tensions between governments and ethnic community. Specifically he stated:

There was a concern that the card could be used for ethnic profiling of particular groups.

We note that, in the original draft of the bill, one of the details on the register was going to be country of birth.

---

<sup>32</sup> Mr Pearce, Liberty Victoria, *Committee Hansard*, 5 March 2007 p73

We were very concerned that that could have led to ethnic profiling and targeting of particular groups, not necessarily by this government but by a future, more nefarious government.

There was always that option or potential, so we were very concerned.

We do note however that on the register there is still the distinction between permanent residents and citizens and that is of great concern to us as well. With the obvious increasing distinction between those groups of people and the government's proposal to raise the threshold for citizenship through higher-level English language testing, there is a concern that permanent residents could also be discriminated against eventually with regard to health and welfare benefits. That potential still exists to a lesser extent with the legislation in its current form.

### **For the right reason**

Clauses 6 and 7 together set out the Government's stated objects and purposes of the proposed legislation. Broadly stated, they are premised on providing a less complex and more convenient method of accessing Commonwealth benefits, reducing fraud, improving access to relief in emergency situations and empowering access card owners to reveal their own personal information to whom they choose.

In terms of privacy laws, purpose governs use. To ensure transparency, accountability and the appropriate exercise of power, the Government's stated objectives need to be tailored specifically to the provision of Commonwealth benefits.

Arguably, as currently worded clauses 6 and 7 should be modified so as to ensure unanticipated uses do not become lawful. The potential exists for function creep to exist most notably in the name of convenience and under the guise of a card owner choosing to reveal their own personal information to whom they choose.

### *Function Creep*

Function Creep is a term which was mentioned on several occasions in the course of the Committee's hearing. This is where the purpose for using smart card technology may be easily extended from the stated objectives and purposes mentioned above to include other purposes.

A good example of past function creep is the Tax File Number. The function of the Tax File Number has moved from, as it was initially, a purely taxation-related function, to the present situation, where it is used to cross match data relating to government assistance of various sorts and superannuation.

The Democrats note that several instances of potential function creep were referred to in the course of the hearings. Function creep could occur by:

- widening the faceprint database to include, for example, digitised images from the proposed Queensland driving licence smart card scheme<sup>33</sup>

---

<sup>33</sup> Ms Scott, Secretary, Department of Human Services *Committee Hansard*, 6 March 2007, p 132.

- allowing the cards to be used to go onto a train, go into 7-11 convenience store and buy a pork bun, or as door access control systems<sup>34</sup>
- permitting a commercial entity to purchase the application licence and the software necessary to allow people to put additional functionality on the individual space of the card<sup>35</sup>
- undertaking analysis of stored biometric photographs using facial recognition technology<sup>36</sup>
- tracking individuals over a period of time to ascertain movement and interaction behaviour<sup>37</sup>
- individual operators could use, unauthorised, the system for their own purposes.

Overseas, in Canada convenience stores are able to swipe drivers licenses through a lottery terminal to verify a customer's age when purchasing alcohol, cigarettes or adult magazines.<sup>38</sup> Colorado is in the midst of scanning every driver license into a database to match against criminal mug shots and currently, the company that brought biometrics to Tampa in 2001, Viisage, has one-third of the market for digital driver's license photos and supports its database with software able to scan 50 million faces per second.<sup>39</sup>

The Democrats believe that function creep is a common problem with all new technologies and cannot be wholly avoided by regulation.

Accordingly, the Democrats consider that there is an obligation on the developers and users of smart card technology to anticipate function creep and to take steps to prevent undesirable forms of function creep from occurring. This should be in the form of specifically prohibiting certain users or purposes, at this time, which can be revisited in the future.

### *Data Matching*

The Department of Human Services Secretary, Ms Scott, in her evidence to the Committee referred to existing arrangements for data matching in relation to the Australian Tax Office and, for example, the Child Support Agency and for parts of data matching between Centrelink and the Australian Tax Office in relation to family tax benefits. However, she denied that there will be any link between the creation of this register and the Tax Office.<sup>40</sup>

---

<sup>34</sup> Evidence of Mr Adam Faulkner, Sony, *Committee Hearing*, 2 March 2007, p 47.

<sup>35</sup> *Committee Hansard*, 6 March 2007, p 53

<sup>36</sup> Federal Agent Drennan *Committee Hansard*, 6 March 2007, p 27

<sup>37</sup> *Committee Hansard*, 6 March 2007, p 22

<sup>38</sup> See Canada: Stores Downloading License Data Could Be Violating Privacy Laws, 12 March 2007 available at <http://www.privacy.org/archives/001939.html>

<sup>39</sup> Surveillance and Social Control - Criminal Justice Research Paper available at <http://www.freeonlineresearchpapers.com/surveillance-social-control-criminal-justice>

<sup>40</sup> *Committee Hansard*, 6 March 2007, p 143.

One of the central privacy risks to this system is the desire for future secretaries and governments to 'weave together' data held in the centralised register with other databases. Having a data warehouse such as the register makes it much easier and more cost effective for the large scale comparison of individuals.

The Federal Privacy Commissioner, Ms Karen Curtis, in discussing Item 14 of the table under clause 17 of the bill (putting a flag against a cardholder's name), warned of the dangers of including any ability in the proposal to facilitate data matching without appropriate oversight. Ms Curtis said in relation to the proposal to flag individuals:

This appears to mean that each agency with which an individual has a relationship must be able to link the individual's access card number and their local agency issued identifier.

This creates a situation where more than one agency can hold a common government issued identifier for a single individual. The risk here is that the ease of matching those records may in the future increase the temptation to change existing restrictions on information sharing between agencies and thus the framework for large-scale data matching could be in place. The best way to ensure that this does not happen is to avoid creating a system that would make it easy to happen.

The Democrats are very uneasy about the possibility of record linkage either internally between the participating agencies or to external databases. It is conceivable, if not now most certainly in the future, that techniques will exist whereby a link, either through the flag, the access card number, the serial number in the chip, or even through the adopted software could facilitate and increase the options for privacy invasion and further fraudulent or inappropriate use.

Several witnesses recognised 'hooks' in the proposed scheme which would allow participating agencies, and others, to go on a fishing expedition trawling through the database. Notably Ms Julia Nesbitt from the AMA stated:

The other protection that we are going to seek more advice on is ensuring that those numbers—the number on the surface and the linking number in the chip—are different.<sup>41</sup>

While the Attorney-General's Department, and others, have stated publicly that there are no current plans to link this database to other databases, to give Australians confidence, that this will not occur the Democrats propose specifically outlawing the linking of the database to other Commonwealth databases and will move an amendment prohibiting this.

Such a step has the support of both the Federal Privacy Commissioner and the Acting Victorian Privacy Commissioner.<sup>42</sup>

---

<sup>41</sup> *Committee Hansard*, 6 March 2007, p 91.

An additional safeguard might also be to legislate to prevent the Secretary having the power to 'bulk release' information from the register and chip, without sufficient cause and independent oversight.

### *Age Eligibility*

Clause 22 of the Act states that in order to be eligible for an access card you must be at least 18 years of age, unless the Secretary of the Department of Human Services exempts you from this requirement pursuant to Subclause 65(5)(a).

The Australian Medical Association has stressed the importance of providing health and social welfare benefits to young people. Specifically, Dr Haikerwal said the age restriction should be lowered from 18 to 15 in the legislation

It is very important that that is reflected in this legislation, so that the young people who often struggle to get health care or do not want to present do not feel that there is another barrier in the way. I do not think that is a particularly major change, but it certainly gives more clarity, especially to younger people.<sup>43</sup>

Mr Bray, of MedicAlert also stated:

A significant thing—I would have kicked myself if I had left and not told you this—is that 26 per cent of our new members writing every month are under 18 and 19 per cent are under 12. You might think Medic Alert is for older people. That shows the care of parents for their children. Health problems are affecting younger people because of allergies—even peanuts are bad—and rising rates of asthma in children. With 26 per cent under 18, and with 18 to 19 per cent under 12, how does the access card go? You do not have a card unless you are 18 or over and you need a government payment, so how does it go looking after them?

In response to the issue of age eligibility the government has merely responded that its current guidelines for determining eligibility in relation to Medicare will apply to the proposed Access card.

The Government's Guidelines setting out an exemption from the age criterion for persons 15 years and older are not good enough while the age barrier of 18 remains enshrined in the legislation.

These Guidelines can be changed or withdrawn by the Government at any time and for any purpose.

The Democrats have an amendment to the legislation to ensure that the age in the legislation stands at 15 and not 18.

---

<sup>42</sup> *Committee Hansard*, 6 March 2007, p 51

<sup>43</sup> *Committee Hansard*, 6 March 2007, p 85

---

*Tracking individuals*

The Government's own submission last month to the Senate inquiry explained that all online activity will be securely logged, including access, authentication, transactions and business activity. All logs will be analysed constantly for anomalous behaviour. The Bill contains penalties for people who inappropriately access information contained in the access card system. (see page 57, section 6.2)

While the Democrats welcome greater accountability through routine auditing of log files, greater precision about what the log files may contain, the regularity of inspection, and release of this information to third parties is required.

As a result of a Question on Notice to the Department dated 27 February 2007, the Department has been able to confirm that audit logs will be retained for audit and security purposes.

Given that law enforcement agencies can compel the Department to provide parts of the log under the search warrant, or the Department is able to provide that information if it falls within one of the exceptions to the disclosure principle contained in the *Privacy Act* (Information Privacy principle 11) the issue of how long these files should be retained is more sharply brought in to focus.

For the first time, it seems the Department of Human Services will not give a guarantee that there will be no analysis of the log files created as a result of a transaction with Medicare, Veterans' Affairs and other participating agencies.

The mandatory retention of the log files potentially gives law enforcement agencies and the Department access to a vast wealth of communications data without a judicial warrant.

I am concerned that log files will be able to be mined by law enforcement agencies and approved agencies. This will be a valuable tool in determining your physical data i.e. were you at a crime scene or were you at your appointment?

I draw my concern largely from the Department's response but also from the evidence of two witnesses before the various Senate hearings.

Ms Irene Graham at the Senate Hearing in Melbourne said:

In the context of the technical and administrative information, we are concerned that audit logs are mentioned. The question is: what exactly is meant by audit logs? A great deal of information in the bill, and even more so in the explanatory memorandum, tends to suggest that the chip on the smartcard is not going to be used for the purposes that most people who know about the technology would expect the chip to be used for—that is, as a storage means that a card reader can read without it needing to be attached to a back-end database. A lot of the information in the explanatory memorandum is tending to suggest that every time you go to the doctor and have to prove that you are entitled to access Medicare the card will have to

be put into a card reader that is linked to the back-end database so as to check the currency of information.

It is looking like these audit logs are going to be a tracking device. Every time a person presents a card it is docked into a reader, so one can fairly easily gain a vision of all the times you use it on a bus to prove that you are entitled to a discount or you use it at the cinema or whatever to prove that you are entitled to a discount—and I am talking about people with age pension discounts et cetera. There is serious concern about what is being set up, either intentionally or completely unintentionally because it has not been thought of. Are we setting up something that will result in so-called audit logs that are a complete history of everywhere a person has been and where they have presented their card voluntarily? Obviously, if it is DHS they need to present their card there. What is meant by audit logs? Is this ultimately setting up a complete tracking and surveillance system? I am quite prepared to accept that possibly the government does not intend to do that, but it is a fact that we know the technology can do it. The information that the government has provided to date provides no indication of how that is intended to be prevented. You cannot help but be left with a perception that this is probably what the outcome will be.

Mr O' Sullivan from ASIO, in response to a question from Senator Lundy about whether ASIO is communicating with the Department of Human Services about tracking of the card's use via the telecommunications system, stated:

If there were legitimate reasons from a national security/counter-terrorism point of view that required us to try to obtain that information, we would do so and we would have done so at any point in the past irrespective of whether this particular card comes into existence. I do not have any reason to believe that the proposition that the existence of this card somehow increases those things has any validity.

The Democrats will move an amendment to the legislation that will ensure deletion of log files in a timely fashion, similar to what occurs with SMS messages in the Telecommunications arena so that this information is recognised for what it is: an ephemeral by product limited in its shelf life".

### *Concession Status*

As mentioned above, the Democrats are concerned at the breadth of circumstances in which the Access card may be required to be produced in order to establish eligibility for a concession. Wherever practicable, use of the card as the means in which to prove concessional status in relation to goods and services should be discouraged. This is merely another example of function creep.

## *In the right way*

### *Timing Drafting and consultation process*

The Democrats note that the proposed Access card legislation before the Senate Committee is a text book study in how not to engage constituents, interest groups, government agencies, regulators, academics, peak bodies.

The Government readily admits at page 63 of its explanatory memorandum that the bill does not deal with all matters relate to the access card. Matters not dealt with in the bill include administrative review, privacy issues, oversight and governance, dependants, carers and other linked persons, suspensions and cancellations of registration, replacement of lost and stolen cards, the transition period between 2008 and 2010, protection of information, the individual's area of the chip, computer hacking and requirements to present the card to obtain Commonwealth benefits from 2010.

In practice the Bill is enabling legislation for future matters. The Bill will reserve the Government the right to implement the system with minimal privacy and security protections. The public are being asked to trust the Government that these protections will be afforded in other legislation.

As a result of the evidence presented to the Committee, it was very evident that:

- more individuals with practical experience should be involved in the law making process.
- before drafting the smartcard legislation the department should have attempted a review of all other Commonwealth related legislation that would impact on the proposal, most notably, the *Archives Act*
- issues such as coherence of the proposed bill with subsequent legislation had not properly been thought through
- definitions are unclear and ambiguous
- time frames for the implementation of the proposed scheme have not been developed with care. For example, the Attorney-General's Document Verification Scheme will not be operational until 2010. Registration is not compulsory until 2010.
- there is a lack of harmony between powers which facilitate collection, use and disclosure of personal information and powers which protect personal information from misuse.
- there is an absence for a simplified process for the review of decisions under the proposal, yet a significant portion of this legislation is concerned with various

senior officials such as Ministers and Secretaries making potentially adverse decisions that will affect the rights of Australians .

*Individual area of the chip*

For the reasons mentioned above, it is not appropriate for this legislation to be mandating an individual area of the chip when much of the detail about how much information is to be stored in this area, who will have access to this information and at what cost remains unknown.

Clause 33(a) should be omitted from the current bill.

*Consent and Opportunities to choose*

Clauses 40, 41 and 57 of the Bill expressly state that card owners may choose or consent to use their card, for such lawful purposes they choose, including copying.

These clauses must be read aside one of the stated purposes of the legislation which is to permit card owners to use their card for any lawful purpose they choose.

Consider first the situations in which the legislation mentions where individual's have a choice: the presenting of the card for identification purposes, in relation to their own area of the card and the taking of a photocopy of the card.

In these situations it is easy to see how an individual may be pressured in to allowing Commonwealth and State agencies access to information for all manner of purposes. Arguably, in the area of Commonwealth and State Government service provision the individual will have no meaningful choice; the individual's only available alternative will be to forgo any Commonwealth or State benefit.

The Democrats can envisage the situation where Commonwealth and State Government agencies and the private sector will offer Australians the following deal: cooperate and sign the consent form or be deprived of the benefit.

Within a few years of the card operating it is also likely that consent will become 'standardised.' Ms Anna Johnston in her evidence warned:

The bill says that copying information from the card is allowed with the person's written consent. We imagine that it will not take very long for the banks, the RSL clubs, the Video Ezys, Qantas and so on to simply have your written consent printed on your application form or your entry form. It will just be written into standard terms and conditions.<sup>44</sup>

---

<sup>44</sup> Ms Anna Johnston, *Committee Hansard*, 5 March 2007, p. 25.

The Democrats' worries about consent not being informed, voluntary and specific enough are also shared by the Federal and Victorian Privacy Commissioners. Ms Helen Versey, Acting Victorian Privacy Commissioner stated:

Having worked in many areas of the law for a long time, I am conscious that consent is a very difficult area. The law talks about true consent being informed, voluntary, et cetera. But much consent actually is not really consent at all, and it gets more difficult the more vulnerable and the less educated people are.

People assume that because a government body is asking them for something, it is required. I can give you an example. Every year or two years, Australia Post send out a massive survey asking for all sorts of personal information. It is completely voluntary; you are entering a competition if you fill it out. But I can assure you that every time it goes out, our inquiry lines are full of people who believe that it is compulsory because a government organisation has asked them for the information and they believe they have to fill it in. That is one example where, even though it is apparently completely by consent and voluntary, people do not understand that and believe that they are obliged to produce the information.

The other side of the coin is that you can coerce people into giving their consent through, say, benefits. For example, let's say that the Queensland government wants to put its drivers licence onto your part of the card. Because they do not want to run two systems, it is much more convenient and financially viable for them to have it on your part of the card. But it is supposed to be your choice—you consent to whatever goes on the card. Then they make it financially beneficial for you to have your drivers licence on the card. They give you incentives to do it, or it becomes much more convenient to do it. So you can either produce your card as a form of identity, say, or you have this terrible and difficult process to go through to show your identity. Those are examples of what I mean by 'coerced consent'. You may not be expressly asked or forced to do it—or even impliedly forced to do it—but the alternative may be too arduous, so it is much more convenient to do it, even if you do not particularly want to.<sup>45</sup>

Ms Curtis stated:

I am concerned that individuals may not always be aware of the potentially significant longterm privacy risks when they are asked for their consent, especially where they may be offered an immediate and tangible convenience.

My office suggests that organisations should not be permitted to copy or record the access card number with or without the individual's consent

---

<sup>45</sup> Ms Helen Versey, *Committee Hansard*, 5 March, p. 17.

unless it is in accordance with the specific requirements of other legislation.<sup>46</sup>

The Democrats agree with the Privacy Commissioner's sentiments that where individuals are being asked to make a choice, to give their consent, or choose a course of action, it must be a real and not illusory choice.

### *The Technology*

The law alone cannot ensure that the right balance is struck between privacy, security and convenience.

A number of submitters commented on the possibilities with this new technology. Stephen Wilson, of Lockstep remarked:

There is a rich and untapped vein of privacy enhancing potentials in this technology, which are not yet apparent.

These potentials could be implemented right away or they could be retrofitted later, but only if the legislation allows.

I believe there is a huge opportunity to protect Australians' privacy using this technology, but it may be lost if the bill prematurely freezes the design of the chip, and I will come back to that.

This opportunity may indeed be lost if we do not have state-of-the-art privacy protections from day one when the system is released.<sup>47</sup>

While the Democrats are not in favour of technological determinism as a guiding force for regulation, it must be acknowledged that technical feasibility necessarily plays a central role in attempts to regulate any media.

Where technology does have a role to play the Democrats encourage, wherever feasible, the adoption of privacy enhancing technologies.

The current proposal provides little detail on the design of the card, the reader, and chip technology.

The Democrats note the disappointing response received from the Department in relation to our question: "Has the government examined the possibility of matching individual's personal information on the card rather than against a central register which would negate the need for information to ever leave the card? If so, why has the option been dismissed?"

---

<sup>46</sup> Ms Karen Curtis, Federal Privacy Commissioner, *Committee Hansard*, 6 March, p 42

<sup>47</sup> *Committee Hansard*, 6 March 2007, p 56

While the Department replied that it has investigated a variety of models for the implementation of the Access card, it has not confirmed whether this privacy enhancing model was contemplated.

Whatever technology is chosen, designing, developing, testing, and evaluating the card and reader system needs to be done properly. This will take time.

Where technology can deliver on the proposed outcome and be privacy enhancing it should be encouraged. For example, technical access controls to simply shut a person out of a database.

### *Offences*

Although there is some statutory protection of personal information stored on the surface of the card, the register and the chip against unauthorised disclosure and misuse, the proposal has several shortcomings.

In the limited time that the Committee had to consider this Bill, the more worrying features of the offence provisions are:

- they provide only incidental protection against unauthorised use or disclosure of cardholder's personal information. Essentially inappropriate access and disclosure is left for referral to the areas of current privacy, criminal, or employment laws. Of course, such referrals are dependent on the organisation which has done something wrong doing something about it or alternatively telling an affected person where to go for help.
- the legislation only provides for criminal sanctions against the offenders, without conferring any right to civil remedies upon the victim. More significantly, they do not protect against the 'authorised' use and disclosure of personal information.
- all Commonwealth and State employees could be immune from prosecution for wrongly requiring a person to produce an Access card or wrongfully copying information from the Card.

The Democrats do not believe that the Government fully appreciates the risks of unauthorised disclosure with such a honey pot of information.

The Democrats will seek to amend the legislation to require those affected by a privacy breach involving this proposal be notified of when the breach occurred and what the agency has done to remedy the breach. The presumption should be to notify, unless certain circumstances apply.

Stronger precautions against potential misuse are needed. Otherwise the benefits will disappear if the Government loses the trust and confidence of customers, staff and citizens.

### ***At the right time***

For reasons mentioned throughout this supplementary report, the Democrats are of the view that now is not the appropriate time to be legislating for smartcards.

Greater consultation and guidance is required. The issue would benefit from the formation of an expert multidisciplinary panel to examine the complex issues which cut across the technical, legal, cultural and privacy divides.

The Government should learn from its mistake of leaving privacy matters out of this Bill to be dealt with later. It may prove to be a costly exercise. What would have been far more reasonable would have been to release its Privacy Impact Assessment to demonstrate that privacy was being factored into all decision making processes.

It is generally accepted that the reasons for completing a Privacy impact assessment are to enable public bodies to make informed choices early in the design phase of any major project in respect of what information should be collected, the manner of collection, usual disclosures and data security.

Where privacy is considered early it will often be the case that a privacy enhancing solution will be no more difficult or costly to implement than an intrusive one.

### **Conclusion**

The Bill in its current form is both unworkable (for the technical reasons discussed above) and undesirable (due to its impact on rights and freedoms, and because of its failure to give Australian citizens confidence that the Government has properly costed and future-proofed this proposal).

The Bill is likely to have a major effect on the development of the smartcard infrastructure in Australia and therefore requires closer analysis than a rushed three day Senate Committee hearing.

**Senator Natasha Stott Despoja**

March 2007

# **AUSTRALIAN GREENS ADDITIONAL COMMENTS AND RECOMMENDATIONS**

## **Introduction**

The Australian Greens support the committee recommendation. The enormous number of problems and threats to privacy and human rights posed by the bill require more detail and time for the Australian people and Parliament to evaluate the proposed access card.

The issues outlined in the main committee report must be addressed if the government is to have any hope of convincing the public that the benefits of the access card are greater than the dangers.

However, even if these suggestions are implemented, the Australian Greens remain opposed to this legislation as it will still enable, for the first time, a central national database of information on all Australians to be held by government.

In particular, the unwarranted access of police and security agencies to the database poses a great danger to democracy and freedom.

There also remains the danger that over time the access card will become an ID card.

The Australian Greens will support the changes implied in the report as they would significantly reduce the threat to privacy of all Australians posed by this legislation.

The Committee report calls for a range of matters to be considered by the government when drafting a consolidated bill. The Australian Greens believe that the matters raised need to be changed rather than just considered.

Therefore the Australian Greens make the following recommendation:

## **Recommendation 1**

**That if the access card proceeds, it be amended to ensure that**

**- the provision of appropriate terminals or readers to those agencies and providers providing benefits and services to access card holders be included in the budget for the proposal;**

**- the only mandatory information displayed on the surface of the card is the card holder's name and that other information displayed is at the discretion of the card holder;**

**- the Commonwealth area of the chip store existing agency identifiers and that these numbers are used when linking a card to a participating agency database,**

**rather than the access card number, removing the requirement for agency linkage to a central database;**

**- the form and manner in which the register is to be kept is set out in legislation and prohibitions such as keeping the register separate from other data bases are expressly stated;**

**- the following determinations are made by way of legislation or disallowable legislative instrument:**

**what proof of identity (POI) information and documents are needed for registration (clause 13(2));**

**when applying for an access card, what 'other specified information' or documents that the secretary deems necessary: (i) to be satisfied of the applicant's identity, or (ii) to obtain information required for the card or the register (clause 23(2)(b), and**

**- any proposals to appoint additional participating agencies are made through legislative amendment of the principal act.**

It is clear from evidence to the Committee and the character of the proposed legislation that despite the extensive public relations effort by the government it is in fact intended that the access card will become a national ID card.

Ms Johnston from the Australian Privacy Foundation told the Committee at the Sydney hearings that, 'The access card is an ID card by design and by effect'.<sup>1</sup>

Evidence to the committee showed that the Access Card is far more extensive and intrusive than Labor's Australia Card proposal which was rejected by the Australian people and the then Liberal opposition.

The Committee received as a submission an article by Professor Greenleaf, the Co-Director of the Cyberspace Law and Policy Centre in the Faculty of Law at the University of New South Wales. The article was published in the Computer Law and Security Report. Professor Greenleaf compares the Australia Card to the access card and concludes:

In most respects the privacy dangers of the new ID system are worse than those of the Australia Card.<sup>2</sup>

The article also includes tables of comparison between the Australia and access card. They indicate that the privacy dangers associated with 18 features of the two cards are the same, the privacy dangers associated with 14 of the features of the access card are

---

1 *Committee Hansard*, 2 March 2007, p. 14.

2 Graham Greenleaf, *Australia's proposed ID card: still quacking like a duck*, Science Direct, Computer Law & Security Report, Elsevier Ltd 2007, p. 166, provided in *Submission 43a*.

worse than those proposed in the Australia Card, one feature cannot compare and one feature of the access card was better than the Australia Card proposal.<sup>3</sup>

The government has not been honest about its intention. It is clear it wants a national ID card but, because of public opinion is unwilling to say so.

As a result the legislation has been drafted with an enormous amount of discretion invested in the Minister and the Department of Human Services Secretary. In all there are 29 clauses that empower the Minister or the Secretary to determine the form and structure of the access card scheme, what information can be collected and who can use the information.<sup>4</sup>

We note that it is likely that this bill would be in breach of any Bill of Rights or Human Rights Act if one was in existence in Australia as in the United States or the UK.

### **Additional Issues and Recommendations**

As outlined in the committee's main report there has been little time to examine all issues of concern regarding the access card. Outlined below are some of the additional concerns and recommendations of the Australian Greens and which have not been covered in detail in the report.

#### ***Police and ASIO***

Citizens' rights to be free of unjustified surveillance and attention by security agencies are the mark of a free and democratic society.

History shows that national identity cards and systems are often associated with authoritarian regimes because they are able to be used to control the population.

It is not surprising therefore that much concern about the access card has been centred on police and intelligence agencies access to the national database. This has included comments by a government backbencher that the card failed "the Nazi Test".<sup>5</sup>

It became apparent during the committee hearings that the AFP and ASIO already enjoy extensive access to Human Services databases and that such access would continue under the access card scheme.

It is astonishing that police and intelligence agencies access to such an extensive national population database would only be regulated by the individual decision of an administrative official.

---

3 Graham Greenleaf, *Australia's proposed ID card: still quacking like a duck*, Science Direct, Computer Law & Security Report, Elsevier Ltd 2007, p. 164, provided in *Submission 43a*.

4 *Submission 35*, pp. 8-13.

5 *The Australian*, 7 February, 2007.

While police must gain a warrant to search homes in this case they would only need the say-so of the Secretary of the Human Services' Department to examine extensive personal information, perhaps much more revealing than what is in your bedroom or kitchen.

The Australian Greens believe that if the access card proposal proceeds access to such information for use in criminal or intelligence investigations must require at least as rigorous scrutiny as is required for other intrusions on individual privacy and other rights by police or intelligence agencies.

It is still unclear exactly what access State and Territory police services would have to the national database and whether they could require a person to produce their card. However it seems that their powers would be similar to those of the Australian Federal Police.

## **Recommendation 2**

**That if the legislation proceeds it should be amended so as to require ASIO, AFP and State and Territory police to obtain a warrant from a judicial officer before accessing information held in the access card register (database).**

## **Concessions**

Evidence to the committee suggests one-third to a half of card holders will not be able to have their concession status visible on the card; including young people, students and many people with disabilities. This will mean any business and government agency that wishes to issue a concession-priced service will need card readers.

Evidence to the committee showed that the impact on concession eligibility and the practical use of concessions have not been properly assessed. The government was unable to explain exactly how many card readers would need to be issued to, or purchased by, businesses and State government and other federal government agencies.<sup>6</sup> We still do not know what impact this will have on the willingness of businesses and services to continue to offer concessions. We still do not have information about the impact of this proposal on the workability of concessions in a range of settings, including public transport and commercial outlets, such as cinemas.

The Australian Greens are concerned that additional burdens on business and users will reduce the availability and use of concessions.

---

6 An additional submission by the Office of the Access Card received late in the Committee process suggests at least 50,000 readers will be needed but is unclear if these are only for government services and medical practitioners. See *Submission 39a*, p. 11.

## **Young people**

The Australian Greens welcome the acceptance by the government that young peoples' access to medical services should not be further restricted by the introduction of the access card. We share the concerns of the Australian Medical Association about the detrimental impact of such a restriction.<sup>7</sup>

But we are waiting to see amendments to the legislation to ensure a young person does not require parental permission to obtain a card, as operates now with Medicare, before being satisfied that the government is not using the access card to prosecute a conservative moral agenda.

How children and young people will interact with the card still seems extremely undefined. Evidence to the committee by the Secretary of DHS revealed the department may be considering an additional card especially for young people. To our knowledge this is the first time this had been raised in public.

## **Blind and vision impaired**

There is a range of concerns relating to vulnerable groups of people and those with special needs that have not been addressed by the government in the design of the access card.

In particular, those who are blind and vision impaired would be significantly disadvantaged by the current design of the card, which is not distinguishable from other cards.

The Australian Greens support the following recommendation of Blind Citizens Australia who gave evidence to the inquiry:

[That] [t]he access card be distinct in its size, shape, tactile and visual appearance to enable people who are blind or vision impaired to distinguish it from the mass of cards people who are blind or vision impaired use in their daily lives. These specific needs for the blind and vision impaired community should be commonly embedded features applied to all cards.<sup>8</sup>

## **Recommendation 3**

**That if the access card proceeds it should be distinct in its size, shape, tactile and visual appearance to enable people who are blind or vision impaired to distinguish it from the mass of cards people who are blind or vision impaired use in their daily lives**

---

7 *Submission 38*, p.3

8 *Submission 58*, p. 6.

## **Emergency Medical Information**

The government has attempted to sell the access card to the public by extolling the benefits of the cardholder's 'part of the chip'. One of the uses for this part of the chip could be to hold medical information on the person which could be used in an emergency.

It is clear, however, from evidence to the Committee that there are large problems and health dangers from promoting the card as a source of emergency medical information.

There are concerns that such information would not be a reliable substitute for existing practices of assessing the patient and accessing patient records. Doctors could not rely on the information as it may have been altered by a patient or not accredited in the same way as other information.

Currently a major source of emergency medical information is provided through the issuing of emergency emblems or bracelets and accessing a national register maintained by the not-for profit Australian Medic Alert Foundation. Over 260,000 Australians currently have important medical information held by Medic Alert which is accessible to health professionals via a 24-hour hotline.

Evidence to the Committee suggests that the access card, while not being able to replace the service supplied by Medic Alert, could undermine the viability of the Medic Alert service and lead to a reduction in reliable information available to medical professionals in an emergency. In the words of Mr Bray, Australian Medic Alert Foundation, in evidence to the Committee, '[w]ithout authentication, the health alert on the card can be so misleading that it can be dangerous'.<sup>9</sup>

### **Recommendation 4**

**That emergency health information not be stored on the card.**

### **Copying the Card**

The bill makes it an offence to copy information on the surface of the card, but not the information on the chip or in the database. This is a significant omission, particularly given the admission by the Secretary of DHS during evidence to the Committee that a deliberate decision was made to omit such an offence.

If the access card proposal proceeds, the Australian Greens believe that it should also be an offence to copy information on the chip or in the database.

Graham Greenleaf, *Australia's proposed ID card: still quacking like a duck*, Science Direct, Computer Law & Security Report, Elsevier Ltd 2007, p. 166, provided in *Submission 43a*.

### **Recommendation 5**

**That if the legislation proceeds it should be amended to include an offence prohibiting the unauthorised copying of information on the chip or in the database.**

### **Keeping of scanned documents**

The Committee heard from several witnesses about their concerns about the storing of proof of identity documents in the central database.

The Australian Privacy Foundation in its submission to the Department of Human Services on 12 January 2007 writes that, 'the copies of so-called "proof of identity" documents represent the raw materials needed for identity theft'.

The Committee heard how this would make access to the database more appealing for people seeking to engage in identity theft and that if such people did gain access to the central database the carrying out of identity theft would be made much easier because of the presence of identity documents.

The Australian Greens do not support the storing of scanned copies of proof of identity document in the central database and therefore make the following recommendation:

### **Recommendation 6**

**That if the legislation proceeds it should be amended to remove any capacity for scanned proof of identity documents to be kept and stored in the central database.**

### **Alleged Financial Savings**

A number of wildly diverging claims have been made by proponents of the access card for the savings to government revenue and the reduction in fraud that might be possible as a result of the scheme.

While it is impossible to properly assess these claims, not least because of the refusal of the government to release its business case for the card, it is clear that substantial arguments can be made that the card could also increase fraud and identity theft.

The Australian Privacy Foundation in evidence to the committee stated that the Access Card 'is a solution looking for a problem. I would argue that is not a good

enough reason to spend \$1.1 billion in an almighty hurry or to put Australians at increased risk of identity theft'.<sup>10</sup>

It is still unclear from evidence to the Committee to what degree claims for a reduction in fraud are based on the current use of concessions by out-of-time or underage ID as opposed to large scale defrauding of the Commonwealth.

Evidence to the committee highlighted the threat of increased identity theft and the possibility that the development of a single form of identity could facilitate identity fraud as much as reduce it.

It is clear that all systems are incapable of being totally secure from hacking or fraud. The Australian people deserve to know that the system will be as secure as it can be.

Yet evidence to the committee from the Defence Signals Directorate who will be advising on the security of the project has said they are unable to assess the security of the card because the project is too undeveloped.<sup>11</sup>

Parliament should not be expected to sign off the creation of the access card with the issues of fraud and security unresolved.

## **Conclusion**

The Greens remain opposed to the access card proposal and this legislation.

The access card must be opposed for the same reasons John Howard gave for opposing the Australia Card in 1987 when he said:

... so we've come down against the present ID card, for three fundamental reasons: the first is the enormous invasion of privacy, the second is that the savings and the advantages of it are not great, and thirdly and most importantly, the cost of it...

The access card proposal is so riddled with problems and threats to privacy that there are no doubt improvements can be made.<sup>12</sup> The Australian Greens will seek to move amendments to do this.

However the fundamental core of the proposal, a universal card and a national population database, so threatens Australian's human rights that it must be rejected.

## **Senator Kerry Nettle**

---

10 *Committee Hansard*, 2 March 2007, p. 15.

11 *Submission 59*, p. 2.

12 See, for example, the suggested amendments by Professor Greenleaf in *Submission 43* and the Australian Privacy Foundation *Submission 30*.

# **ADDITIONAL COMMENTS BY SENATOR FIERRAVANTI-WELLS**

## **Access Card - Inquiry Into Human Services (Enhanced Service Delivery) Bill 2007**

There may be benefit in the Committee's recommendation that this bill be combined with the proposed second tranche of legislation for the access card system into a consolidated bill as it will enable the important concepts of security and privacy protections to be considered in their entirety alongside the benefits the access card will provide. However, having regard to the evidence provided in submissions many of the concerns expressed by the Committee have already been addressed in the current legislation and the Committee's report fails to give due regard to the benefits of the access card in its proposed form in meeting its stated purposes.

A primary concern of the Committee has been whether there is a potential for the access card to evolve into an national identity card in the event that a biometric photo, signature and a unique number are visible on the face of the card. As the Committee itself noted the Government has explicitly declared in Clause 6(2) of the bill that "access cards are not to be used as, and do not become, national identity cards." The protections contained in the bill are sufficient to allay such concerns.

The Committee's concerns with respect to the features to be included on the face of the access card, in particular the inclusion of a photograph, fail to take into account important evidence on the purpose for the inclusion of such features.

In this regard particular note should be made of the public submission provided by KPMG which stated at page 17:

The rationale for having the photo on the face of the card is fundamentally about a person being able to simply and quickly prove who they are in a number of service outlets. One of the platforms of the entire HSS initiative is a strengthened POI and a capacity to authenticate a user, identify their entitlements (such as concessional status) and ensure they have access to the right services and benefits.

The capacity to authenticate a user must be applied across the entire DHS, DVA service system including providers such as allied health workers, GPs, pharmacists and ambulances, who for the first time, will have access to volunteered information about a persons emergency contact details. Being able to simply and quickly identify the cardholder is paramount in these circumstances.

KPMG has attempted to design a system on a card reader platform that will facilitate uniform access by the full range of DHS and DVA providers. Therefore, whilst pharmacists and GPs might have card reading technology

capable of photographic identification, not all providers in the system will. If DHS design a system of access and entitlements based on who has a card reader capable of photo identification and who does not, the system will be forced to slip back into different standards and different business rules. The system again becomes unpredictable and confusing for consumers.

Also, whilst the card won't be required by people outside the DHS service system as POI, a consumer may choose to use it to prove their identity in other environments such as accessing a transport concession, joining a registered club, applying for a passport, or obtaining airline tickets.

Finally, KPMG considers that greater trust in the overall system will be strengthened by considers(sic) being confident that their card can not be used by someone else. Having a photograph on the card and all the other securities in place, in our view, is likely to strengthen that confidence.

The Committee Report ignores the fact that even if readers capable of electronically reading a photograph were available in all service delivery outlets, which in itself may not be possible, there would continue to be a number of situations in which readers would not be available for use:

- During electricity blackouts and when systems are down;
- Natural disasters; and
- 'In home' and remote location service providers (eg Doctors)

On the basis of the above, the inclusion of a photograph and other personal information on the surface of the card as proposed is necessary as it will provide a unique and highly flexible method of ensuring accurate service delivery.

Evidence heard by the Committee also established the importance of the inclusion of a photograph and other personal information on the surface of the card as being essential security measures in reducing the fraudulent abuse of the health and welfare systems and in minimising the prevalence of identity fraud and theft. These are important protections for cardholders and also ensure that entitlements flow only to those who are eligible.

The combination of "on card surface" and "in chip" security elements along with the modular design of distinct databases will also constitute a significant improvement over current systems and will ensure the suitable protection of cardholder information.

The stated intention of the access card is to streamline the delivery of government services. However, it is also important that recognition be given to the community's desire that the card also provide personal utility beyond the immediate needs of government. This card represents a platform for the facilitation of government service delivery into the future and in the form proposed, will be sufficiently flexible to meet the changing needs of individuals.

---

The merits of the access card as proposed by the Government were well articulated by the Sydney Morning Herald in its editorial of 14 March 2007 which stated:

The Federal Government's planned access card is already attracting opposition of a predictable kind from privacy groups. Their concerns are understandable, but so is the Government's need to streamline and secure access to welfare and other benefits, including Medicare payments. For recipients of such benefits - and that means virtually every Australian - the card should make life easier. Its primary function, the elimination of welfare fraud, will also save taxpayers money - \$3 billion over 10 years, say the Government's consultants.

.....

Outside government, the card cannot be demanded as identification. Within it, each agency will only be allowed access to a given individual's files with that agency. Those decisions are prudent, and should provide further reassurance. Worries about identity theft can never be entirely eliminated, even by the most secure encoding methods - but the **access card** is far more tightly regulated than the existing plethora of identity cards for government benefits, all of which have been making the identity thieves' work simpler.

The **access card** will always be a trade-off between administrative efficiency and individual rights and security. There is no single correct answer to the questions it raises. If implemented, it will most likely be a source of occasional controversy as governments seek to alter what it does. In that respect, it is like many of society's laws, regulations and institutions that inhibit individuals' freedom. On balance, however, we believe its benefits outweigh its dangers. The **access card** deserves support.

**Senator Concetta Fierravanti-Wells**



# Appendix 1

## Submissions Received

<b>Submission Number</b>	<b>Submitter</b>
1	Michael Skeggs
2	Kevin JR Murphy
3	Victor M Lambe
4	Robert H Bromwich
5	Datacard South Pacific
6	Name Withheld
7	Margery Street
8	Gavin Street
9	Festival of Light
10	Humanist Society of Victoria
11	Mr Stephen Brown
12	Australian General Practice Network
13	Kerry Baker
14	David Bath
15	Name Withheld
16	Benjamin D McGinnes
17	Brian Rowe
18	Ms Graham
19	GW & GL Manley
20	Confidential
21	Margaret McKay
22	Vision Australia
23	Women's Health Victoria
24	Warren Holland
25	Austroads
26	Robert W Parry FCA
27	N Phillips
28	ACT Government

29	New South Wales Council for Civil Liberties Inc (NSWCCL)
30	Australian Privacy Foundation
31	Laurie Phillips
32	Australian Smartcard Users Forum
33	Department of Veterans' Affairs
34	Students' Representative Council University of Sydney
35	Liberty Victoria
36	Department of Premier and Cabinet Government of Western Australia
37	Australian Electrical and Electronic Manufacturers' Association Ltd (AEEMA)
38	Australian Medical Association (AMA)
39	Australian Government
39a	Australian Government
40	Ken Cuming
41	Access Card No Way Campaign
42	Consumers' Health Forum of Australia
43	Cyberspace Law and Policy Centre
43a	Cyberspace Law and Policy Centre
44	Public Interest Advocacy Centre (PIAC)
45	Lockstep Consulting Pty Limited
46	Office of the Privacy Commissioner
47	Health Issues Centre
48	Office of the Victorian Privacy Commissioner
49	Sexual Health and Family Planning Australia
50	Australian Bureau of Statistics (ABS)
51	NSW Commission for Children & Young People
52	Australian Bankers' Association Inc
53	Electronic Frontiers Australia Inc
54	Access Card Consumer and Privacy Taskforce
55	Aboriginal and Torres Strait Islander Social Justice Commissioner on behalf of the Human Rights and Equal Opportunity Commission

56	Abacus – Australian Mutuals
57	Cedric Hingee
58	Blind Citizens Australia (BCA)
59	Department of Defence – Intelligence & Security
60	David Tones
61	Australian Lawyers for Human Rights
62	Alastair Kinloch
63	Non-Custodial Parents Party
64	The Finance Sector Union of Australia (FSU)
65	Dr Michael Head
66	The Royal Australian College of General Practitioners



## **Appendix 2**

### **Additional Information and Related Evidence**

- 1 Answers to Questions on Notice received from Attorney-General's Department
- 2 Answers to Questions on Notice received from Department of Human Services
- 3 Answers to Questions on Notice received from Australian Privacy Foundation
- 4 Answers to Questions on Notice received from Public Interest Advocacy Centre
- 5 Answers to Questions on Notice received from Victorian Privacy Commissioner
- 6 Answers to Questions on Notice received from National Archives
- 7 Answers to Questions on Notice received from Australian Federal Police
- 8 Answers to Questions on Notice received from Consumer and Privacy Taskforce
- 9 AUSTRAC Advice

### **Related Evidence**

Answer received from Department of Human Services in response to a question on notice from Senator Stott Despoja at Supplementary Budget Estimates 2006-07



## **Appendix 3**

### **Public Hearings and Witnesses**

**Friday, 2 March 2007 – Sydney**

BERRY, Ms Carol Gaye, Solicitor, Public Interest Advocacy Centre

BOLTON, Mr Bill, Senior Enterprise Architect  
Computer Sciences Corporation

COOK, Mr Christopher, Vice President  
Computer Sciences Corporation

GREENLEAF, Professor Graham William, Private capacity

HARTLAND, Ms Kerri, Deputy Secretary  
Department of Human Services

JOHNSON, Ms Kathryn, General Counsel  
Department of Human Services

JOHNSON, Ms Marie, Chief Technology Architect  
Department of Human Services

JOHNSTON, Ms Anna, No ID Card Campaign Director  
Australian Privacy Foundation

JORDAN, Mr Christopher David, Partner, KPMG

SCOTT, Ms Patricia, Secretary  
Department of Human Services

SIMPSON, Mr Michael, General Manager, Policy and Advocacy  
Vision Australia

SUMAKTAS, Ms Ebru, Officer, Policy and Advocacy  
Vision Australia

TOMLINS, Prof. Ron, Chair, National Standing Committee on Quality Care  
Royal Australian College of General Practitioners

WESTACOTT, Professor Jennifer Anne, Partner  
Leader Government Practice New South Wales, KPMG

WILSON, Mr Stephen, Managing Director, Lockstep

**Monday, 5 March 2007– Melbourne**

BELL, Mr David Peter, Chief Executive Officer  
Australian Bankers Association Inc.

BRAY, Mr Hedley Murray  
Australia MedicAlert Foundation

BURKE, Mr Anthony John, Director  
Australian Bankers Association Inc

FISHER, Ms Michelle, Manager, Policy  
Office of the Victorian Privacy Commissioner

GRAHAM, Ms Irene Joy, Executive Director  
Electronic Frontiers Australia Inc

MATTIAZZO, Ms Nadia, Executive Officer  
Blind Citizens Australia

MESSIMERI-KIANIDIS, Ms Voula, Chair  
Federation of Ethnic Communities Councils of Australia

O'ROURKE, Ms Anne, Vice-President  
Liberty Victoria

PEARCE, Mr Michael, SC, Vice-President  
Liberty Victoria

POWER, Mr John, National Policy Officer  
Blind Citizens Australia

RICHES, Mr Graham, Immediate Past National Chairman  
Legacy

SHARP, Mr David, Legal Coordinator  
Access Card No Way Campaign

VAN VLIET, Mr Peter, Executive Officer  
Federation of Ethnic Communities Councils of Australia

VERSEY, Ms Helen Kathryn, Acting Victorian Privacy Commissioner  
Office of the Victorian Privacy Commissioner

WARNER, Mr Timothy, Convenor  
Access Card No Way Campaign

**Tuesday, 6 March – Canberra**

ALDERSON, Dr Karl, Assistant Secretary, Criminal Law Branch  
Attorney-General's Department

BYRNE, Ms Sarah Elisabeth Catharine, Legal Counsel  
Australian Medical Association

CURTIS, Ms Karen, Privacy Commissioner  
Office of the Privacy Commissioner

DRENNAN, Federal Agent Peter, Acting Deputy Commissioner  
Australian Federal Police

EVANS, Ms Sheridan, Assistant Secretary, Identity Security Branch  
Attorney-General's Department

FARR, Mr Gregory Douglas, Second Commissioner of Taxation  
Australian Taxation Office

FELS, Professor Allan, Chairman, Consumer and Privacy Taskforce

GODWIN, Mr Des, Director, Identity Security Branch  
Attorney-General's Department

GRANGER, Ms Jennifer Anne, Second Commissioner of Taxation  
Australian Taxation Office

HAIKERWAL, Dr Mukesh Chandra, President  
Australian Medical Association

HANKS, Ms Verity, Senior Legislation Officer  
Australian Federal Police

HARTLAND, Ms Kerri, Deputy Secretary  
Office of Access Card, Department of Human Services

HUGHES, Ms Joan, Chief Executive Officer  
Carers Australia

JOHNSON, Federal Agent Ray, Manager, Special Operations  
Australian Federal Police

JORDANA, Mr Miles, Deputy Secretary  
Attorney-General's Department

MCKAY, Mrs Robyn, Acting Deputy Secretary  
Department of Families, Community Services and Indigenous Affairs

NESBITT, Ms Julia, Director, General Practice and E-Health Department  
Australian Medical Association

O'SULLIVAN, Mr Paul, Director-General  
Australian Security Intelligence Organisation

PILGRIM, Mr Timothy, Deputy Privacy Commissioner  
Office of the Privacy Commissioner

ROBINSON, Mr Geoffrey, Deputy Commissioner  
Australian Taxation Office

SCOTT, Ms Patricia, Secretary, Office of Access Card  
Department of Human Services

SHEEDY, Ms Joan, Assistant Secretary, Information Law Branch  
Attorney-General's Department

SOLOMON, Mr Andrew, Director, Policy  
Office of the Privacy Commissioner

SPIERS, Ms Carolyn, National Manager, Access Card Group  
Department of Veterans' Affairs

SULLIVAN, Mr Mark, Secretary, Department of Veterans' Affairs

TELFORD, Mr Barry, General Manager, Policy and Development  
Department of Veterans' Affairs

THOMPSON, Mr Andrew, Director, Intelligence  
Australian Taxation Office

YATES, Mr Bernie, Deputy Secretary  
Department of Families, Community Services and Indigenous Affairs

