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.[1] 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.

[1] 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;[2]
- its non-release of its KPMG report in relation to the Access card proposal;[3]
- 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…[4]

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.

---

[2] *Committee Hansard*, 2 March 2007, p52.

[3] *Committee Hansard*, 2 March 2007, p 12.

[4] 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.5 ('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. [6]

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.

[5] See www.privacy.org.au

[6] See Australia's proposed ID card: Still quacking like a duck , Professor Graham Greenleaf, Volume 23, Issue 2 , 2007 available at 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. [7]

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.[8] 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 bout $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.[9]

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."[10]

---

[7] 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.

[8] Committee Hansard, 2 March 2007, Sydney, p11.

[9] Committee Hansard, 2 March 2007, Sydney p25. See http://www.sirca.org.au/news/releases/2003/0302FraudBook.html

[10] 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.[11]

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. [12]

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.[13]

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

[11] http://www.theage.com.au/polls/form.html

[12] See National Identification Cards available at www.privacyinternational.org

[13] 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[14] 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.[15]

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.

[14] See http://www.dutchnews.nl/news/archives/2007/01/

[15] 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 card16
- it is likely that in at least 50% of cases staff matching people to the photos in the card will make an incorrect match17
- 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 theft18

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

[16] 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

[17] 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

[18] 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. [19]

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[20]

- 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.'

---

[19] 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; "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.

20 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

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 [21]
- 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[22]

---

[21] 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

[22] 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[23]
- agencies who sell bus tickets[24]
- agencies who sell movie tickets[25]

[23] Ms Kathryn Johnson, Department of Human Services, Committee *Hansard, 6 March 2007* p117.

[24] As above

[25] As above

- the local video shop[26]
- a pharmacist [27]

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.

[26] Ms Helen Versey, *Committee Hansard,* 5 March 2007, p. 8.

[27] 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.[28]

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 proposal29,
- 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.30

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.

---

[28] For example, the Anti-Terrorism Act 2005 (Cth)

[29] Mr O'Sullivan *Committee Hansard,* 6 March, 2006 p13

[30] 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 Ac*t 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*.[31]

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.

---

[31] 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.[32]

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.

[32] 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 occassions 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[33]

[33] 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[34]

- 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 [35]

- undertaking analysis of stored biometric photographs using facial recogniion technology[36]

- tracking individuals over a period of time to ascertain movement and interaction behaviour[37]

- individual operators could use, unauthorised, the system for their own purposes.

Overseas, in Canada convenience stores are able to swipe drivers licenes through a lottery terminal to verify a customer's age when purchasing alcohol, cigarettes or adult magazines.38 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.39

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.[40]

---

[34] Evidence of Mr Adam Faulkner, Sony, *Committee Hearing* , 2 March 2007, p 47.

[35] *Committee Hansard,* , 6 March 2007, p 53

[36] Federal Agent Drennan *Committee Hansard*, 6 March 2007, p 27

[37] *Committee Hansard*, 6 March 2007, p 22

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

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

[40] *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.[41]

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. [42]

---

[41] *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 elgibile 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. [43]

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 are 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.

---

[42] *Committee Hansard*, 6 March 2007, p 51

[43] *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 concened 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 cad 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 complusory until 2010.
- there is a lack of harmony between powers which facilitate collection, use and disclosure or 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 proposol, 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.[44]

[44] 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.[45]

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

[45] Ms Helen Versey, *Committee Hansard*, 5 March, p. 17.

> unless it is in accordance with the specific requirements of other legislation.[46]

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.[47]

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?"

---

[46] Ms Karen Curtis, Federal Privacy Commissioner, *Committee Hansard*, 6 March, p 42

[47] *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 that 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