health and social services

Access Card

Consumer and Privacy Taskforce

Report Number One

Chair, Professor Allan Fels, AO

September 2006

ACCESS CARD CONSUMER AND PRIVACY TASKFORCE

ADVICE TO MINISTER FOR HUMAN SERVICES

Report Number One

ISSUES AND RECOMMENDATIONS IN RELATION TO ARCHITECTURE QUESTIONS OF THE ACCESS CARD

The Hon J Hockey MP
Minister for Human Services
Parliament House
CANBERRA ACT 2600

Dear Minister

I am pleased to submit *Advice to the Minister : Report Number 1* from the Access Card Consumer and Privacy Taskforce.

Following the release of our *Discussion Paper Number 1* on 16 June 2006 which called for submissions, I am pleased to report that almost 100 such submissions were received. In addition members of the Taskforce have undertaken a programme of consultations with over 110 individuals, groups, organisations, representatives and government departments across Australia. The input from the submissions and consultations have helped shape our final views and recommendations.

Report Number 1 focuses upon issues related to the architecture of the proposed Access Card and the attendant supporting systems.

On behalf of the Taskforce I would like to thank the officers of the Department of Human Services, the participating Agencies and your Office who have assisted us in the provision of advice related to our inquiry and report. I would further like to acknowledge the support received from Mr Benjamin Battisson of the Office of Access Card who has acted as our Executive Officer.

I commend the report to you.

Yours sincerely,

Professor Allan Fels AO

Chairman

Access Card Consumer and Privacy Taskforce

25 September 2006

TABLE OF CONTENTS

INTRODUCTION

The Consumer and Privacy Taskforce was established in May 2006 by the Minister for Human Services to report to him directly on consumer and privacy issues arising from the Government's announced plans to introduce a new health and social services Access Card as a replacement for 17 existing health and welfare entitlement cards [see *http://www.humanservices.gov.au/access/additional_information.htm*].

The Minister for Human Services appointed Professor Allan Fels AO to chair the Taskforce. Professor Fels is the former Chair of the Australian Consumer and Competition Commission and currently Dean of the Australia and New Zealand School of Government.

Professor Fels thereafter selected two Taskforce members who have particular experience and expertise in matters of privacy and consumer rights to assist him. These two members are: Professor Chris Puplick AM (a former New South Wales Senator and NSW Privacy Commissioner) and Mr John T D Wood (a former Deputy Commonwealth Ombudsman and Director of the Federal Bureau of Consumer Affairs). The Taskforce has been assisted by Mr Benjamin Battisson of the Office of Access Card as its Executive Officer.

Although the Taskforce has a primary responsibility to provide independent advice to Government, it conducts its proceedings in as open and public a fashion as possible. It sees itself as having a clear mandate to reflect to Government the views which are put to it during its community consultation and through the process of receiving submissions, regardless of whether those views support or oppose the Government's proposal. It will augment any such reporting on community views with its own opinions and advice. It intends not only to respond to specific requests by Government for advice, but also to be positive and proactive in offering its own advice to Government whenever it feels that this is appropriate. It will of course be giving advice conscious of the Government's basic policy decisions, its implementation programme and especially its timing so that Government decisions can be made with the benefit of that considered advice.

In June 2006, the Taskforce published a Discussion Paper which outlined the Government's stated case in support of the Access Card project and which canvassed the major issues which it saw as arising from those proposals. In the Discussion Paper the Taskforce explored all the issues which it saw as critical to an understanding of the Government's proposals for an Access Card. It also outlined a number of Key Issues for further discussion and resolution.

The Discussion Paper invited Submissions to be lodged by 27 July 2006. Some 104 submissions were received. At the end of August the Taskforce published the majority of those submissions on its web page, withholding only those where the submitters asked that their submissions be not published for commercial-in-confidence or personal reasons. Nevertheless the Taskforce has listed all submissions received as an Appendix to this Report.

Submissions were received from most of the significant privacy, consumer and civil liberties organisations and bodies in the welfare, medical, pharmacy and banking sectors. A limited number of submissions were received from individuals. The Taskforce received few inputs from those people who might be characterised as the principal intended beneficiaries identified in the government's proposals.

In addition, members of the Taskforce undertook extensive direct consultations with both submitters and other interested and/or expert parties and with relevant government Departments and Agencies. These included the Department of Human Services, Medicare Australia, Centrelink, the Child Support Agency and the Department of Veterans' Affairs in several locations across Australia as well as Departments such as Foreign Affairs and Trade, Attorney-General's, Finance and Administration, Immigration and Multicultural Affairs and agencies such as the Australian Taxation Office, the Australian Electoral Commission and the Australian Bureau of Statistics. Some 120 such groups or individuals were involved in these discussions in all States and Territories. Details of these are also listed in this Report.

It should also be noted that the Taskforce has adopted a number of underlying principles throughout our recommendations. First, we believe that all decisions about the Access Card should be made in as transparent a fashion as possible with a maximum degree of public consultation and explanation. The establishment of the Taskforce itself is an important means by which a significant part of that transparency can be achieved, and its own recommendations are based on its views concerning the critical importance of transparency.

Secondly we have assumed that the Government will want to adhere to the new series of guidelines released in September 2006 by the Office of the Privacy Commissioner and the Attorney General which serve to inform businesses of their privacy obligations. It is our assumption that the Government would want to bind itself to the same standards as it is urging on the private sector. (see http://www.privacy.gov.au/)

Thirdly we have sought at all times to see what the Access Card programme can do to enhance customer benefits with particular reference to the extent to which this initiative can improve the ease and efficiency of interactions between public and government agencies, protect them from the risks of being the victims of fraud and/or identity theft and ensure that burdens of compliance (for example in initial proof of identity requirements or later requirements to produce the Access Card in order to obtain entitlements) are minimised.

Finally we have sought to find ways in which new technologies can be developed or used which will themselves be privacy enhancing. In this regard we are conscious of the point urged upon us by the Submission from the Office of the Privacy Commissioner that there is a difference between a technology being genuinely privacy enhancing rather than just less privacy intrusive. Where technology can help guard against fraud – especially by preventing it in advance rather than simply detecting it after the event, or where it can be used to minimise the amount of personal data otherwise collected and held – the Taskforce is highly supportive of its use. We have no doubt that there are many new and emerging technological developments which can strengthen consumer choice and privacy protection. In our analysis of the various solutions put to us, we have sought to balance the enhancement

of customer choice and control with the need to improve government efficiency in operations and service delivery and with the need to protect privacy.

We have adopted a general approach in this Report of not identifying (except in particularly relevant circumstances) the individual Submissions from which we have highlighted or adopted suggestions. The decision to highlight or adopt suggestions is something which derives from either the relevance or the utility of those suggestions and is thus unconnected with their source or origin. Where the Taskforce has adopted any such suggestion it has indicated this endorsement. Otherwise, where it has come to its own position or conclusion, it has also stated this clearly.

The Taskforce has been given significant scope to raise with the Minister matters which we regard as germane to the whole Access Card project not narrowly confined to technical questions of consumer benefit or privacy protection. The Taskforce expresses its appreciation to the Minister for the latitude he has allowed it in developing its advice to him.

In this respect we would also acknowledge the exceptional level of support and co-operation rendered to the Taskforce by all government departments and participating agencies. In various Departments we have met with senior officers responsible for such matters as identity management, security and data protection and the development of e-government. In the participating agencies we have had the opportunity to meet with their most senior managers and to observe their operations at the coalface where the chance to talk with front-counter staff was particularly valuable. We have been able to observe the considerable efforts which they are making to provide the best service to customers and to be respectful of the need to maintain their privacy.

AN ACCESS CARD NOT AN IDENTITY CARD

The Taskforce notes the Government's assurances that the Access Card is not intended, nor should be permitted to develop into a national identity card by stealth. The Australian people have clearly indicated that they do not wish this to occur.

It is upon this assurance that the Taskforce has proceeded with its work, and developed its recommendations. These would have been qualitatively different had we been addressing a situation in which a national identity card was proposed or contemplated.

It is vital that public policy be developed which recognises explicitly that there is a qualitative difference between a card needed to authenticate identity for health and social service purposes and one needed to prove identity for such matters as international travel or to assist in law enforcement.

From this recognition flow a number of consequences. For example questions about when the Access Card must be produced, to whom it must be shown and the penalties for its misuse will reflect its status as a health and welfare card, not an identity card. Similarly, this distinction goes to the heart of such matters as the level of proof of identity which will be needed to establish an initial entitlement to be issued with an

Access Card which itself will be the subject of major examination in our forthcoming Registration Discussion Paper.

While this report uses the term "Access Card" throughout, this is purely a generic term as the actual "name" of the Card is yet to be determined. In several of our consultations there emerged some confusion about the use of this term and it is important to clarify the point that the card itself is required not to ensure "access" to services but rather to authorise and facilitate the payment of benefits. People without a card – for whatever reason – will not necessarily be denied access to services to which they are entitled, (especially in the medical environment) but they may be unable to claim the benefits or rebates associated with these services except in exceptional circumstances. Once the Access Card is issued it needs to be held securely by individual cardholders and not be regarded as an easily replaced or disposable document.

The Taskforce's consultations among representatives of the Indigenous community drew our attention to the almost standard practice whereby people "park" their Medicare cards with community health clinics/centres or pharmacies, and the need which will arise to educate people not to do this with their Access Cards which they will need to produce for Centrelink and other purposes. At least in the interim period as familiarity with the need for and operation of the Access Card develops, policies will need to be in place to allow "access" in the absence of an Access Card.

DEVELOPMENT OF THIS SUBMISSION TO THE MINISTER

After consideration of the submissions and the input from our consultations, the Taskforce came to a number of preliminary and draft conclusions and identified a number of issues about which it felt that it needed further advice. These were discussed with the Department of Human Services and the Lead Advisor (Booz Allen Hamilton) and relevant advice was received.

REPORT TO THE MINISTER AND THE TASKFORCE'S FURTHER PROGRAMME

In this First Report to the Minister for Human Services, the Taskforce wishes to present its Findings and Recommendations in relation to questions going to the fundamental architecture of the Card and the basic operation of the Card system. As we have stated, we have been able to consult with the Department and the Lead Advisor (Booz, Allen, Hamilton), but have not yet had the opportunity to talk to the recently appointed Legal Advisors (Minter Ellison) nor the Chief Technology Architect (Ms Marie Johnson).

During the course of our considerations it became apparent that there were a number of matters related to the difficult question of concessions, the eligibility for many of which flow from possession of certain Commonwealth health or welfare entitlements. Some of the complexities arise from the fact that these concessions are determined (in part) by State, Territory or Local governments or by the private sector. It is not easy to establish the full details of all of these across all jurisdictions. As a result, in relation to the concessions system, the Taskforce is making only limited recommendations to the Minister at this stage, and may return to this question in more detail at a later date.

The Taskforce does not wish to develop any of the major issues related to the Registration process, at this stage. The registration process will be critical to the success or otherwise of this entire undertaking and will be the subject of a further Discussion Paper to be issued publicly in November. However, before that paper can be prepared the Taskforce needs to undertake a considerable programme of further investigations and consultations.

After the issue of the Registration Discussion Paper, the Taskforce will undertake a further round of calling for submissions and engaging in community consultations before presenting a subsequent report to the Minister in the second quarter of 2007.

From there we intend to proceed to the development of a third Discussion Paper which will address the question of the on-going governance and supervision issues associated with the Access Card programme. It will be important to canvass the roles which may be played by existing statutory offices such as the Office of the Privacy Commissioner, the Human Rights and Equal Opportunity Commission and the Commonwealth Ombudsman and the operations of their respective legislation, together with discussing the need for any other mechanisms for public accountability and effective oversight of the programme.

THE GOVERNMENT'S CASE FOR THE CARD

This is an area in which the Taskforce thinks it appropriate to restate the Government's case for the Access Card as we presented it in our initial Discussion Paper.

The Government's argument for a new health and social services Access Card

The key objectives of the Access Card programme are to better facilitate the access of consumers to health and welfare services to which they are entitled. It will also provide greater assurance that people do not obtain services to which they are not entitled.

The Government believes that the current system for accessing health and social service benefits is overly complex, often inconvenient for many Australians (especially those most in need of assistance) and is exposed to unacceptable risks of fraud.

The Government aims to meet these objectives by establishing:

- a smart card based infrastructure that enables enhanced customer services and improved efficiency; and
- a robust customer identification and registration process, placing emphasis on prevention and detection of fraud.

Without robust proof of identity to verify eligibility, measures that merely cut red tape and improve access for consumers would fail to eliminate weaknesses in the present

system (such as identity fraud problems which are undetected currently) and not deliver the benefits to the community that the Government is seeking.

The form of the Access Card

The Government is proposing that:

- the Access Card will be a plastic card incorporating an electronic chip to hold information and security features additional to those which appears on its face or reverse
- on the front there will be the cardholder's name and photograph
- on the reverse there will be the cardholder's number and digitised signature
- in the chip there will be other details to help authorised agencies to facilitate the cardholder's access to benefits or entitlements, together with the opportunity for each cardholder to add certain information which they want to have recorded. The chip will hold details of addresses, concessional status, children and other dependents or carers' responsibilities
- separate from the card, there will be a Secure Customer Registration Service (SCRS). This SCRS will hold a limited amount of information to allow verification of the card itself and updating of customer details such as address, new entitlements, changed dependents etc. The SCRS will not contain detailed customer records which will continue to be held separately by Centrelink, Medicare Australia, Veterans' Affairs and other participating agencies.

What the Access Card will NOT be

The Government has stated that the Access Card:

- will not be a national identity card or any version of a national identity card
- will not be compulsory for every Australian
- will not be an electronic health record, that is, it will not contain extensive clinical health information
- whilst there will be no use of biometric fingerprints or retinal scans, the card will incorporate other information, specifically a photograph and a digital signature
- will not be compulsory to be carried at all times or to be shown to anyone other than for the provision of Australian Government health and social services benefits
- the creation of the Secure Customer Registration Service (SCRS) will not result in the amalgamation of existing agency databases. The SCRS will be established separately from participating agency databases and will not contain any sensitive agency specific information
- participating agencies will not have access to other agencies' information as a result of the implementation of the Access Card.

Who will need the card?

The Government has stated that:

- only those Australians who wish to receive certain government benefits will need to have the Access Card to obtain those benefits.
- the Access Card will be used to access benefits administered by Department of Human Services agencies (including Medicare and Centrelink) and the Department of Veterans' Affairs (DVA).

When and how will people get an Access Card?

The Government's plans are that:

- commencing in 2008 and running until 2010 there will be a registration programme inviting all Australians to obtain an Access Card, although some pre-registration facilities may be developed to assist consumers in this process
- people will be able to attend various locations throughout Australia to register for and obtain an Access Card where they will need to provide proof of their identity by using certain specified documents.

The Taskforce understands that the Government's case for the introduction of the Access Card in relation to enhancing customer service may be summarised as follows:

> *The replacement of numerous cards held by individuals (and involving 17 cards in total) by one single high integrity card will make transactions with the government easier, faster and less complex. The possession of a single card will reduce the need for frequent re-establishment of both identity and eligibility. An enhanced SCRS will allow for individuals to change or update data in a single operation with seamless flows through into other relevant agencies. Consumers will have enhanced choice about how they use their single card in other circumstances and for other transactions. The payment of emergency or disaster relief will be made easier. The Access Card could become an entry portal into more comprehensive dealings with the government via on-line services and other e-government functions.*

The Taskforce understands that the basis of the Government's case for the Access Card in terms of privacy protection/enhancement may be summarised as follows:

> *The Government believes that the card also offers opportunities for privacy enhancement. These enhancements are based on the proposition that reliable proof of identity and the improved access control this permits are essential components of any effective system to protect personal information held in large databases. Security requires that data is not disclosed to a person misrepresenting his or her identity and that false or misleading data are not included on a person's file.*
>
> *The Government sees the capacity of the Access Card programme to give more reliable identification of customers arising from two sources: the initial registration of cardholders and their capacity to verify the card more reliably, particularly by reference to the SCRS. The verification of existing cards that give access to health and social service benefits depends heavily on visual checks of paper, cardboard and simple plastic cards, some with magnetic stripes. Verification of these existing cards is becoming less reliable. The*

> *absence of a photograph on existing cards is a limitation on identity verification and reliance on alternative photographic identifications, such as driver's licences, is not completely reliable, as Commonwealth agencies have limited capacity to independently verify the card or document.*

The Taskforce recognises that the current magnetic stripe technology used in the present Medicare card is now outdated and has proven vulnerable to improper copying in a way which lays the system open to fraud. Better and more advanced technologies are now available which have been proven and developed since the Medicare card system was first introduced over twenty years ago. This new technology is based upon the use of a silicon chip incorporated into a so-called "smart card". These smart cards can contain greater amounts of information (depending on their chip size) thus enhancing their utility and can provide far greater security and protection of privacy than the technologies now in use. Any Government has a responsibility to use the most up-to-date technologies available, consistent with public policies related to costs, efficiency, approved/designated functionality and privacy protection.

In this very early stage of the development of the Access Card programme many of these issues and arguments are neither well developed nor widely understood. The Taskforce is aware that the Government is seeking to develop programmes of community education which will address these concerns, and it is supportive of this initiative.

We are required primarily to make recommendations to enhance the potential benefits to consumers and the protection of their privacy. Equally, we have a clear responsibility to reflect in our report to the Minister the views that have been put to us either by way of submissions on our first Discussion Paper or in our extensive consultation activities.

A significant number of submissions from groups as diverse as the peak privacy and civil liberties bodies through to those more specifically focussed on welfare provision and service delivery have questioned the rationale for the whole Access Card system.

Some groups have studied the Government's proposals as outlined in speeches by the Minister and publications from the Department and the Office of the Access Card, and have rejected the proposal outright as being either "an Australia Card by another name" or "a national identity card by stealth". This is despite the fact that the Government has given repeated assurances that it has no intention to introduce a national identity card.

Others have argued that, to date, the "case for the card has not been made out". In support of this they point to the difficulties they encounter in not having access to the full version of the KPMG Business Case, and in any event, find parts of the released KPMG report questionable. They also assert that the failure to release the Initial Privacy Impact Assessment has compounded their feelings that the case for the Card is not being presented in a full, transparent and coherent fashion.

The Taskforce appreciates that there are still some details of the operation of the Access Card system which need to be determined and that a full presentation of its

merits, as seen by the Government, is not possible until these matters are resolved. Indeed, a similar point is made, in relation to a more extensive proposal for national identity cards in the UK in a recent report by the House of Commons Science and Technology Committee (*Identity Card Technologies: Scientific Advice, Risk and Evidence*). The Taskforce believes that there is a need for the Government to have a programme of explaining its proposals as they are developed and refined.

Further, some welfare and advocacy groups have indicated that while they see some potential benefits in the Access Card system, they would prefer the expenditure of one billion dollars provided for the scheme to go directly to welfare services or improved processes within Centrelink.

The Taskforce also notes that several submissions and presentations which were made drew our attention to the capacity of a variety of technologies to meet the Government's requirements to be privacy enhancing. While the Taskforce is not in a position to give detailed technical evaluation to all such claims, we are nevertheless impressed with the widespread opportunities which clearly exist for this goal to be achieved.

Finally, there have been a number of submissions which have indicated support for the Access Card system as outlined and in some cases these submissions have urged the extension of the operations of the system to cover additional functionalities, especially in the areas of health services and their delivery.

Very few of the Submissions received failed to raise at least some questions about the Card – either in terms of its architecture or in terms of its proposed and possibly future functionality. Whilst the Office of the Access Card representative was able to answer many of these enquiries during the consultation phase, there were still a significant number (for example in relation to possible or potential e-purse functions and the involvement of private sector financial and commercial interests) which were not able to be answered definitively.

The Taskforce recognises that the whole Access Card scheme is in the early stages of its development and so is not surprised to note that there is a level of uncertainty and mistrust in the community about the exact proposals which are being advanced despite the extensive material which is already in the public domain. Addressing this uncertainty and mistrust and clarifying the proposal must be a high priority for Government.

We draw attention to this fundamental issue of trust. Over the period June to September 2006 research for Unisys (undertaken by Newspoll) indicated a 5% increase (to 33% of a sample of 1200 respondents) in people declaring that they were "extremely concerned" about other people obtaining or using their credit cards. Similarly, 31% of respondents were "extremely concerned" about unauthorised access to/misuse of their personal information, an increase of 600,000 people in a three-month period if extrapolated to the entire Australian population.

During the site inspections undertaken by the Taskforce we were able to observe the role which front-line staff play in helping to inform the general public about their rights and responsibilities. We were very grateful for the opportunity to talk with

these staff members, and in the process were able to assess how familiar they were with the Government's proposals for the Access Card to date.

Within these Participating Agencies there is an opportunity for the Government to make use of its own trained and competent staff to explain the Access Card project to members of the public with whom they are in daily professional contact. Provided that they themselves are given adequate information, training and support – and there is obviously some distance to go on this at present – this should be possible to achieve.

Two up-front questions which involve matters of basic policy will need to be addressed before a comprehensive programme of officer and public education is commenced.

Benefits paid by Centrelink are generally the result of initiatives which arise as policy in Departments other than Human Services. In particular, these are the Departments of Health and Ageing (DoHA); Families, Community Services and Indigenous Affairs (FaCSIA); Education, Science and Training (DEST) and Employment and Workplace Relations (DEWR). Many people consulted by the Taskforce expressed a degree of concern that personal information given by them to Centrelink would be transferred to the databases of the agency whose policies were resulting in their payments and generally matched across all government health and welfare agencies. Many people did not understand that all the policy Departments are able to access the relevant parts of the Centrelink database at present.

It was also, rightly, pointed out to the Taskforce that all policy departments and participating agencies (at present) have privacy or confidentiality provisions contained within their specific legislation and that they are subject to the provisions and requirements of the *Privacy Act 1988* and the associated Information Privacy Principles and the control of data-matching legislation. It is also accepted that the operation of the Secure Customer Registration Service (SCRS) itself would be subject to the same standards and constraints.

The Taskforce believes that there is a need for greater reassurance to be provided to Centrelink (and to a lesser extent Medicare) customers about the way in which their personal data is managed, controlled and used. Concerns can arise, for example, when individuals see reports of extensive "data-mining" operations being undertaken between Centrelink and the Australian Taxation Office and the reported employment by Centrelink of "a panel of data-mining specialists" and yet are unaware of exactly why such operations are necessary to protect the public revenue and detect fraud.

The Taskforce is aware, and commends Centrelink, for the production of a number of brochures which detail how Centrelink shares data with other agencies; how it seeks to balance privacy and public interest in its determination about the disclosure of personal information and what its statutory obligations are. It also publishes clear statements in relation to the privacy of missing persons and the way in which it responds to enquiries in this sensitive area.

Even some of the more established advocacy groups seem unaware of the relevant provisions of the Commonwealth *Privacy Act* and the controls in place under the *Data-matching Program (Assistance and Tax) Act*; section 135AA of the *National*

Health Act or conversely the access provisions under section 92(1) of the *Commonwealth Electoral Act 1918*. On the other hand there is little information in the public domain to explain how Public Interest Certificate Guidelines operate and how Determinations are made under legislation such as the *Social Security (Administration) Act 1999* or the *A New Tax System (Family Assistance)(Administration) Act 1999*. These and similar Acts give Ministers the right to delegate to their Departmental Secretaries the right to make Public Interest Determinations which permit the sharing of sensitive personal data among specified government departments or agencies. They involve determinations about matters which are highly privacy sensitive and affect the rights of individuals.

In providing information about the proposed operation of the Access Card system, an opportunity presents to address this question.

The second point which has been put to the Taskforce in numerous submissions is the question of whether there should be two Access Cards and not just one. The Government has stated its policy position to replace up to 17 existing cards with one single card, and the Business Case presented by KPMG was predicated upon this decision.

However, a number of submissions have argued that for those people who are only Medicare cardholders (some 5.5 million people), there is no need for them to receive a card which extends beyond this level of entitlement, while other submissions argue that, as a matter of principle, medical information (Medicare data) should always be maintained separately from any other personal data. It should however be remembered that personal health data will not be held on the SCRS – each participating agency (including Medicare) will maintain personal data on their own separate databases, and these are not linked to each other directly. [This argument is distinct from another which has been put to us regarding the issue of more than one Access Card to the same person so that they can leave one of their cards with their regular health provider - a matter to be addressed in the registration paper.]

The argument for two cards was advanced with particular reference in relation to people who, at this stage, are Medicare customers only. The Taskforce, however, notes the argument put to it that Australia's health and welfare systems are becoming increasingly interwoven and interdependent. This is particularly the case in relation to family and concessional payments. It is also undeniable that over the course of a "lifetime" people will pass in and out of the various health and welfare programmes: perhaps from dependent children to independent (Medicare only) young adults to parenthood and then to aged pensioner or concessional status. In these circumstances there is a strong case that consumer convenience is better served by the operation of a single card.

Further support for such a proposition may be derived from two related observations. The first is that separating the Medicare card from welfare service cards may serve to identify and possibly 'stigmatise" welfare cardholders as compared to Medicare cardholders: an undesirable outcome. Secondly there is a general and proper community expectation that government cards should maximise a degree of inter-operability (a policy which underpins the governments own recently announced

Smartcard Framework) and in time a single Medicare card would morph into this entity.

The Taskforce is inclined to the view that having one card is preferable to having more than one, and further notes that the proposition of having more than one is contrary to current policy. However because of the frequency with which the proposition is advanced, and because of the strength of the argument that the whole Access Card scheme is of only limited benefit to (current) Medicare only customers, the Government should (re-)state clearly its decision and its rationale for this decision.

The Taskforce thus recommends that:

(1) Participating Agencies continue to develop comprehensive programmes to ensure that their staff is well informed about the whole Access Card proposal and that this information is kept up to date on a regular basis.

(2) Participating Agencies further develop written material and website material which will inform interested members of the public and clients of the Agencies about the Access Card project. **(**The Taskforce will be advising the Government further on the question of the Registration process which will necessarily impact upon the adoption of the final timetable for such registration**.)**

(3) in this process, clarification be given about the way in which data provided to Centrelink and Medicare is treated/transferred/shared or made accessible within the rest of the Australian government and the protections which exist in current legislation in relation to such matters.

(4) policy and the supporting rationale be (re-)stated in response to the strongly argued view that there should be two cards issued under the Access Card.

INITIAL QUESTIONS FOR RESOLUTION

As the Taskforce identified in its initial Discussion Paper, there are several important questions which have to be understood before we are in a position to advance the public discussion of the Access Card programme and formulate our recommendations. These questions include:

- how can or should a government ensure that once it has determined that certain individuals should be eligible for benefits that those benefits are paid only to those people identified as having that genuine entitlement?
- can such processes of identification be achieved without any such mechanism becoming a broader national identity system ?
- to what extent can any participation in such an identification system be genuinely voluntary?

The Australian Government commenced paying pensions in 1908 with the passage of the *Invalid and Old Age Pension Act*. Ever since there have been pensions or benefits paid out of public revenues, there has been a need for some form of identification system which ensure that payments are made only to those who are legally entitled to them and that public money is expended only pursuant to law. Some form of identification is required whenever a public benefit is extended to, or a right enjoyed

by some people and not to or by others. For example electors need to demonstrate some form of identification before they are registered so that only those genuinely eligible to vote are allowed to do so. Similarly, passports are issued only after applicants have provided proof that they are entitled to Australian travel documents and the associated protections.

As such, it is self-evident that there needs to be some form of identification to provide a basis for the proper administration of government payments to individuals. The Medicare card itself was introduced as part of the process by which a new scheme for administering the payments for medical services was introduced.

Given that a card appears to be the most simple and familiar means of establishing entitlement for the payment of government benefits, the questions become what sort of card should be introduced, what data should it contain and how should its use be controlled. These are issues for the Taskforce to consider.

A national identity card system would include the aspects of its being compulsory, producible on demand by certain authorities, a requirement for people to carry it at all times, its linkage with a unique identifying number and the fact that it is the sole form of identification recognised by government authorities.

The debate about national identity cards in Australia is one with long historical antecedents. Compulsory forms of national identification have been used in wartime, and Australians were registered under the *National Security Act 1939* and the *National Registration Act 1939* and were given a basic identity card under the 1947 *National Security (Manpower) Regulations* to control aspects of post-war rationing.

However in peacetime their use has not commended itself to the Australian people. A recommendation from the Royal Commission of Inquiry into Drug Trafficking (Stewart Royal Commission 1980–1983) which urged the introduction of a voluntary national identity card was never taken up by government.

Nevertheless, in September 1985 in a statement by the then Treasurer on *Reform of the Australian Taxation System* the idea of a national identity card, to be known as the Australia Card, was proposed. The Australia Card was initially proposed for purposes related to taxation, welfare fraud and immigration control (and was to be administered by the Health Insurance Commission) but grew subsequently to incorporate many other potential uses. This proposal was eventually withdrawn.

Since the lapsing of the Australia Card proposal there has been little further debate about national identity cards until the events of September 11, 2001 and the subsequent terrorist outrages of the Bali bombings and the attacks on the public transport systems in Madrid and London. In this new environment the Australian Government indicated that it was reviewing the possibility of introducing such a system and in January 2006 the Attorney General canvassed the idea of appointing a retired judge or similar figure to review the case for such a move. After further consideration by the government, a subsequent announcement was made by the Attorney General in April 2006 that the government had rejected the idea of having any form of national identity card. This position was restated by both the Attorney General and particularly by the Prime Minister on a number of occasions, including

during the announcement of the Government's intention to implement the Access Card system.

Since the idea of having a national identity card has been clearly ruled out by the Government and according to public opinion polls is not supported by the Australian people either, it becomes important to ensure that the health and social services Access Card does not become, now or in the future, a national identity card by any other name.

There are various ways in which this can be done. There can be legislation passed which prohibits such a development, although legislation can always be changed by future parliaments, but only in the full glare of public scrutiny and knowledge. Such legislation could also be used to prevent the growth of demand for production of the Access Card in other than authorised situations.

Indeed, to become an effective national identity card, certain active steps, such as the introduction of legislation or administrative procedures expanding the Access Card's usage would need to be undertaken by government. Such steps would be open to public scrutiny and parliamentary attention.

It is true to say that obtaining the card will be voluntary and that some people will not need to have a card because they may not readily access any of the benefits associated with it. However, 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.

THE RIGHT TO ANONYMOUS TRANSACTIONS

The Taskforce feels it appropriate to comment on the fact that people in free societies such as Australia's have a right to remain and act in an anonymous fashion in certain areas of their lives should they wish to do so. The famous definition of privacy as "the right to be left alone", especially by government, has particular resonance here. The right to anonymity (and the associated right of "pseudonymity"- the use of an intermediate identifier like an internet chat room name) has been little discussed in relation to the Access Card proposal, and yet it is of vital importance in a free society.

This right is recognised explicitly under the Commonwealth *Privacy Act* in relation to private sector transactions under National Privacy Principle 8.

Such a right has particular resonance in relation to accessing certain health care services. Health authorities have long recognised that there are positive health benefits – to individuals and to the wider community – in a system in which people can receive certain health services (especially testing and counselling) in an anonymous

fashion. It is not proposed that these existing rights or practices be compromised or curtailed.

On the other hand, where benefits must be related directly to eligible individuals and not to others, then an effective means of establishing identity (and thus entitlement) must be established.

The greatest threat to the right of anonymity is an unnecessary insistence upon people always having to "prove" their identity in a system supported by a centralised database. On the other hand, systems which are based upon operations and transactions which are more in the control of the individual, in fact may enhance their capacity to operate anonymously where they so choose, provided such people only exercise their rights to such benefits to which they have a genuine entitlement. The Taskforce supports the right of people to make this choice.

It is also important to restate that possession of an Access Card should never be the only way in which individuals will be able to interact with government even in the health and welfare environment.

In addition, when proof of identity is required to access entitlements or benefits, while the Access Card will be the preferred means of identification, it can never be regarded as the sole method. When cards are lost, readers fail or electrical systems are blacked out or when customers so choose, the Taskforce is of the view that there must always be alternatives available and other forms of personal identification accepted.

CONSUMER BENEFITS

The Taskforce received little in the way of direct comment on consumer benefits from actual or potential health and social service beneficiaries in Submissions or during consultations. It has sought to find the views of potential users of the Access Card in other ways including review of reports from focus groups conducted on behalf of the Government.

The Government has, rightly, put some emphasis on the potential for the Access Card to be of real benefit to the consumers of health and social services. The benefits to consumers may be characterised in three ways:

- benefits in more efficient and productive interactions with the Government's health and social service agencies;
- benefits in potential improvements to security for individuals in protecting them against identity fraud and, provided that the information stored or displayed is kept to the necessary minimum, enhanced privacy protection;
- benefits for other uses of the card chosen by consumers.

In the first category, the Government has stated that the Access Card will make it easier to do business with government by streamlining enrolment and registration processes, allowing single points of contact with multiple agencies, enhancing the capacity to develop on-line services and facilitate faster access to emergency

payments and services. More specifically, the Government believes that the Access Card will:

- reduce the number of cards and vouchers required to access various benefits
- provide that a person only needs to register once for an Access Card, thereby eliminating the need to repeatedly provide the same basic details and identity documents to different health and social services agencies. This will mean less time spent waiting in queues and filling out forms
- eliminate the need to contact multiple agencies to update information – people can change details relevant to all agencies by advising a single agency
- provide quicker and easier access to one-off disaster relief and emergency funds – faster access to these payments
- provide a more speedy and efficient method of issuing replacement cards when these are required, especially when cards are lost or stolen
- reduce identity fraud which often does great harm to the recipients of health and social services benefits where they are the victims of identity fraud and the false claiming of benefits which they are entitled to
- allow consumers the choice of including certain information such as emergency contact details, allergies, health alerts, chronic illnesses, childhood immunisation information or organ donor status.

In the second category, the Taskforce has received suggestions that cardholders could choose to use the card for purposes such as:

- identification in banks, hiring goods, obtaining airline tickets, obtaining personal information from service providers such as telephone companies and in numerous other situations. Younger and elderly people, in many cases, do not have driver's licences to use as a means of establishing their identity. In addition, identification with a driver's licence usually discloses the cardholder's residential address and other information which would not be disclosed on visual presentation of an Access Card. The partitioned chip (see discussion below) could also permit selective disclosure of other information relevant for each particular transaction
- date of birth as an aid to proof of age for young people without other documentation and for older people to verify their age-based concessional status
- validation of concessional status in ways that do not disclose personal information to casual observers, or information not directly relevant to the purchase of concession tickets or receipt of concessions for the wide range of goods and services available from government and private sector sources
- accessing services where proof of identity is required in a way which preserves privacy and security through systems which are protected against unauthorised access and for linkage into other secure databases held by financial and like agencies
- enhancing contacts with health and medical service providers through the provision of limited and verified personal health data into the Access Card system, extending to details of organ donation status, advanced medical directives and emergency contact numbers
- helping customers to identify key personal financial data such as payments eligible under the Medicare safety net arrangements

- a stored value (and reloadable) facility leading to micro-payment operations [the Taskforce however draws attention to our discussion below about e-purse functionality]
- self-entered personal information such as "to do" lists.

The Taskforce notes, however, that almost all suggestions for enhanced functionality were accompanied by caveats regarding concerns about privacy issues.

What cannot be predicted is the whole range of options which might become available over time as technology advances and as consumers become more accustomed to operating in a chip-based or on-line environment.

There is clearly a strong push from the existing providers of financial services to reduce face-to-face contacts with customers and to encourage the use of electronic transactions. Governments are increasingly using chip-based technologies in areas such as public transport where travel "smart cards" are becoming almost the norm.

Most Australian governments have passed some form of legislation to promote and facilitate electronic transactions and to enhance their own provision of e-government services. In June 2006, the federal government released the *Australian Government Smartcard Framework* which is designed, in part to "enhance service delivery, improve user convenience and increase security against identity fraud and theft."

As all of the uses of smart cards and related technology become more ubiquitous and more accepted, the Government must be in a position to respond to increased consumer demand for enhanced functionality through the Access Card system. It will be a significant challenge for any Government to balance these demands from consumers with the need to safeguard the overall integrity of the system and the protection of personal privacy within it.

Some consumer benefits would be available at the outset, such as more efficient interaction with health and social service agencies and voluntary use of the card for identification outside the government sector. However, applications such as those involving voluntary recording of information in the chip raise technical, operational, privacy and other issues most of which will not be resolved when the first cards are issued. These additional functions chosen by cardholders could become available over time as these issues are addressed.

The Taskforce recommends that:

> ***(5) the Government clarify what applications will be available when the first cards are issued. This information should be available as soon as possible and before the issue of the first Access Card. The Government should also outline procedures for consultation and the resolution of privacy issues before any decisions are taken on the addition of any new applications.***

THE NEED FOR A LEGISLATIVE BASIS TO THE ACCESS CARD

There is almost complete unanimity among Submissions and in Consultation meetings that the Access Card scheme must be founded upon specific legislation debated in and passed by the Federal Parliament.

This is a view in which the Taskforce concurs fully and the need for such legislation is one of the principal points of advice which it offers to the Minister.

It should first be noted that there are already various statutes in place which seek to guarantee the right to privacy and which establish independent mechanisms for the enforcement of those rights and the resolution of disputes. These statutes are both general (such as the *Privacy Act*) or may be more specific (eg relating to the use of the Medicare number or Tax File Number (TFN)). There are also legislative controls on data matching and the exchange of data between governments and government agencies. In other words, previous privacy protection measures have been expressed in statutory form. The Government has not indicated that its proposal will result in any weakening or compromising of those existing arrangements.

The Government's proposal however clearly introduces some new elements into our health and social services systems, some of which are not yet clearly understood or appreciated in all their ramifications.

It is important to determine the extent to which, if at all, the operation of the new Access Card system should be established by way of legislation, making clear the permitted and prohibited uses. Legislation can be beneficial to the extent that it involves public debate and transparency. On one hand, it may also be the most appropriate way in which penalties can be established and enforced. On the other hand, a legislative scheme may have unforeseen consequences. For example, it may lack the flexibility and timeliness which may be necessary for such a new system to operate with the greatest degree of efficiency or be able to cope with future consumer demands or usages. The system design should not, unnecessarily, prevent uses of the card which would benefit consumers.

However, the arguments in favour of establishing the Access Card scheme on a sound legislative basis are overwhelming. In the first instance, it needs to be recognised that the Access Card marks a significant departure from the traditional way in which Government interacts with a large number (in effect the vast majority) of its citizens, and that the creation of Australia's first national photographic database is likewise an entirely new development. Such profound changes should not be left without legislative debate and authorisation.

Secondly, for the Access Card scheme to operate there must be a significant degree of public trust and confidence in the scheme and in its administration. In the absence of appropriate legislation it is more difficult for this trust to be engendered, developed and maintained.

Thirdly, as most Submissions have noted, both the purposes of the Access Card and its uses need to be defined clearly. Concomitant with this, prohibited uses and penalties for improper use need to be defined, as do related issues such as the ownership of both the Card itself and the data held; the rights of personal access to and correction of one's own record; and the possible personal remedies for improper access and usage by third parties. Such matters cannot be defined without a legislative basis.

Fourth, since there will always be the possibility of the Access Card acquiring more functions over a period of time, either the prohibitions on "function creep" or else the mechanisms for its positive authorisation need to be stated transparently. Again, this should be done only by legislation and we discuss "function creep" in the next section of this Report.

Fifth, the Government has stated clearly that the Access Card is not intended to be or become a national identity card. Legislation has a strong role in ensuring that this assurance is given legislative validation.

Sixth, legislation could make it clear that the failure to present the card is not, in special or exceptional circumstances, necessarily a barrier to the receipt of services – in exactly the same way that currently the physical presentation of the Medicare card is not a prerequisite to accessing treatment. Legislation could also guarantee that other forms of identification are acceptable in the absence of production of the Access Card itself.

Finally, the Access Card system is potentially a complex system which will interact with several pieces of Commonwealth legislation in the health, welfare, taxation, privacy, law enforcement, consumer rights and security fields. It would be useful for all of these to be integrated into one clear and contemporary piece of legislation so that the operation of the proposed system can be understood clearly by reference to only one source of authorisation. At present, to understand fully the legislative basis upon which all the various health and social service schemes and entitlements work is an exceptionally complex undertaking. Different pieces of legislation for example contain quite different privacy and secrecy provisions while legislation in other federal government agencies (for example taxation, immigration, law enforcement) may be relevant. Consolidation, or at the very least, clear cross-referencing to other legislation, would be of great consumer benefit.

The Taskforce is not in a position to provide a definitive statement or list about what matters should be comprehended in legislation. Clearly this is a matter for consultation within Government and across Departments. It is also a matter which should have reference to any relevant recommendations made in the initial PIA.

Legislation itself should, in the opinion of the Taskforce, clearly address at least three broad issues:

- the card itself: with special emphasis on defining prescribed and proscribed governmental purposes and either limiting function creep and/or providing the transparent mechanism for adding new functionality to the card, distinguishing governmental and customer-driven initiatives

- the information to be collected
- the operation and control of the database.

A more exhaustive list could include (inter alia) mechanisms to address the following issues either directly or by appropriate cross-referencing of other legislation:

- clear statement of the purposes of the Access Card
- definition of circumstance in which the production of the Access Card is necessary or required (a model exists in relation to the Privacy Commissioner's responsibilities under section 17 of the *Privacy Act* to regulate the use of Tax File Numbers)
- prohibitions on the demand for production of the Access Card
- definition of information to be held on any database, including the card itself
- cardholders' rights (access, inspection, correction, addition of personal information, information about access by other parties, ownership, redress, recompense, etc.)
- the establishment of a genuine and meaningful system of informed consent whereby data providers know about and understand any authorisations which they are giving for the sharing of that data (and noting the recent comments by the federal Privacy Commissioner regarding the existing system of reliance upon printed Privacy Notices where these are not genuinely understood by people whose consent is being sought)
- data security principles (audit trails, random audits of access, etc.)
- penalties to be imposed for improper demands for production/accessing information or misusing information relevant to the Card
- procedures for authorising enhanced use of the Access Card at some future date through transparent legislative means, preventing function creep by purely administrative decision
- the right of individual cardholders to add data or possibly functions to their own cards which could be specified in a way which ensured that such accretions did not compromise the basic integrity of the Access Card, the system or the rights of other cardholders
- recognition or prohibition of right of access by third parties under existing legislation (e.g. law enforcement and security agencies)
- a comprehensive list of where data from the Access Card system can be exchanged or matched with other government departments, agencies or databases
- control of requests for any future data matching or research investigations
- access to de-identified statistical data by organisations such as Australian Bureau of Statistics (a position supported from a consumer perspective on public policy and interests grounds by the Taskforce)
- the interaction of related legislation (for example new requirements under the *Anti-Money Laundering and Counter Terrorism Funding Bill* proposed as successor to the *Cash Transactions Act*)
- conformity with all requirements under the Commonwealth *Privacy Act* in relation to the coverage and operations of both the Information Privacy Principles and the National Privacy Principles. [The current *Privacy Act* has current limitations which may prevent it from being able to deal comprehensively with all aspects of the Access Card system – for example

its provisions do not cover the operations of State Governments nor small businesses. In addition, the proposed review of the Act by the Australian Law Reform Commission will not be completed until at least March 2008]

- administrative oversight of the Access Card scheme (role of federal Privacy Commissioner, Ombudsman, independent body, etc.).

Any such legislation would, as a matter of course, also include provisions for Regulations to be made, not inconsistently with the Principal Act, to cover other matters which may subsequently arise.

A constitutional issue was raised with the Taskforce in relation to the extent to which Commonwealth legislation could be prescriptive against the activities of State authorities such as the Police or concession verifying bodies. The Taskforce is clearly in no position to comment on the Constitutional issues other than to seek advice from the appropriate Commonwealth authorities. It does however respond to this challenge by suggesting that this matter might be resolved either by seeking a reference of the appropriate powers by the States and Territories (Constitution section 51 (xxxvii)) or by having the matter raised and resolved at a meeting of the Council of Australian Governments (COAG).

The Taskforce needs to bring to the attention of the Government the concern expressed both in submissions and consultations about access to the Access Card database by security and law enforcement authorities. This concern was widespread and ranged from the concerns of privacy and civil liberties groups, to professional associations and community and ethnic representatives. The extent to which this access is already well established is not understood or appreciated and there is a widespread belief – contrary to fact – that Police Services, in particular, are able to undertaking "fishing expeditions" through people's personal health and social services data. The introduction of a new database and system gives the Government an opportunity to address these community concerns. This can be done by specifying the conditions under which such access is granted and ensuring that all such access is upon a lawful basis.

Our recommendations about prohibited access are coloured by experiences in some Australian jurisdictions where issues of unauthorised access have had damaging consequences.

It is important to bear in mind that there are also arguments in favour of not being overly prescriptive or limiting of the legislative basis of the Access Card. Issues of future functionality arise here and cannot be ignored. In the first Taskforce Discussion Paper, we drew attention to the public policy issues arising in relation to legislation including the need to balance the public policy benefits of approved future functionality against the need to restrain "function creep".

We do however make a strong recommendation that additional governmental use functionality should not be conferred on the Access Card without some form of legislative authorisation.

The history of the United States social security number (SSN) illustrates its extension from a very limited social welfare purpose to an extensive, almost ubiquitous

identification system by a series of Executive (i.e. Presidential) Orders without legislative consideration or approval.

In the submission from the Office of the Privacy Commissioner our attention was drawn to the similar development which took place in relation to the Canadian Social Insurance Number (SIN) whose extended use developed without parliamentary oversight. Quoting from a Canadian Parliamentary report, the OPC noted that :

> "Apart from inappropriate use of the number, its uncontrolled use leaves Canadians vulnerable to serious breaches of their personal privacy that range from data-matching carried out without their knowledge and authorization, to identity theft."

There are doubtless other issues which may be appropriate for legislation which will emerge as a result of further consideration and debate, and there are many of these raised in the various Submissions now before the Taskforce.

The Taskforce cannot be prescriptive about this, at this stage, although it would value the opportunity to be involved in any such considerations of a legislative framework for the Access Card.

In the meantime, the Taskforce recommends that:

(6) a comprehensive legislative framework be developed for the Access Card scheme; and

(7) suggestions received in Taskforce submissions and the views of the Taskforce itself be taken into account as these are developed.

FUNCTION CREEP

The Taskforce has referred on several occasions to the need to be careful about how the Access Card might start life as simply a means of facilitating better services to customers in the health and social services sector, but then grows or morphs into something unintended. This process is what we have characterised as "function creep" and it is perhaps useful for the Taskforce to state its views on this subject more explicitly as we did in our original Discussion Paper.

The classic example of function creep is the driver's licence. Driver's licences were originally introduced to do nothing more than to indicate that a certain person was permitted to be in control of a certain type of motor vehicle on public roads – nothing more. Today the driver's licence has evolved into something entirely different and is used for a variety of purposes which have nothing to do with motor vehicles. In many cases, it has assumed, incrementally many of the characteristics of a comprehensive identity card.

Similarly, the cash transactions reporting system expanded to cover a far greater range of financial transactions than was originally intended, and indeed it became necessary for the Government to introduce new legislation to authorise this expansion, and indeed to indicate that even further expansion is contemplated.

Great care will need to be taken to specify the exact purposes for which the Access Card is to be introduced, but equally to specify the purposes for which it cannot be used. In between the poles of express usage and express prohibition lies a grey zone. Excessive rules about prohibited uses, may for example, limit rather than expand consumer control over the Access Card's usage. There are clearly possibilities that consumers will want to expand the role of the Access Card and their rights should not be unnecessarily curtailed.

Although the Secure Customer Registration Service will be established separately from the databases administered by participating agencies, its existence may place greater pressures on Government to expand data-matching exercises. Either such expansion must be prohibited, or else clear and transparent rules must be established to address this issue.

Similarly, issues will arise in time as other cards come into use. There may be for example, cards related to electronic health records or childcare services and there are already a range of entitlement cards issued by State and Territory Governments. It is likely that demands will be made by consumers in the name of convenience for all of these to be linked. The federal, state and territory governments need to be clear and open with the public about how they will address such matters.

Other third parties, such as doctors, pharmacists, health researchers, child protection authorities, missing persons registers and others may also seek to make cases that additional usages or access rights would enhance the welfare of individuals and the community. Again, there needs to be an open and transparent method of dealing with such access requests.

In determining questions about the architecture and functionality of the new Access Card the Government will need to make a certain number of decisions, some of which may be irrevocable. A decision made now about the technology which would physically prevent any such further developments for many years, may or may not be sound public policy. In the first instance, there may be genuine customer demand for new functions to be added. Some of these may relate to the activities of the participating agencies themselves, for example access to details of an individual's own Medicare safety net entitlements, or they may relate to other departments or agencies. The question here is whether consumer demand may drive function creep. The Taskforce believes that the question of whether an enhancement of functionality is driven (or mandated) by the Government or initiated and promoted by the customers themselves is a critical one.

Secondly, there may be additional benefits which might be available or provided in areas not previously contemplated where the use of the Access Card would be the most efficient approach available.

In the absence of outright prohibitions, the issue is not whether additional functions could develop for the Access Card, but the means by which any such additional functions should be considered and decided: by stealth, by incremental function creep or by a process of open and public debate.

THE OWNERSHIP OF THE ACCESS CARD

A suitable matter to be addressed in legislation might be the question of who actually "owns" both the data in the SCRS and the Access Card itself. In the opinion of the Taskforce it would be desirable that the cardholder, that is each individual Australian, should own the card and the associated personal data which they are required to provide.

Current Medicare cards carry the statement that "this card remains the property of Medicare". The Taskforce believes that an Access Card which individuals own will make the whole scheme more palatable and would enhance both consumer sovereignty and potentially enhance privacy protection. It would also give greater choice to individuals about the uses to which they might chose to put the card other than for health and social service purposes and limit the scope for government to make decisions about this without their knowledge or consent.

It may be appropriate to place some limitations on this principle, for example by way of prohibiting individual cardholders from altering or defacing their cards, much as is currently provided in relation to possession of the currency. Such altered or defaced cards could legislatively be deemed to be invalid.

The Taskforce believes, nevertheless, that there is a prima facie case that the Access Card should be "our" card, not "their" (the government's) card.

The Taskforce recommends that:

> ***(8) the Government clarify that matter of who "owns" the Access Card and desirably vest this ownership in the individual cardholder subject to some limitation on inappropriate usage as suggested above.***

DISABILITY FEATURE

There is a strong case for the Card itself to be manufactured in such a way that people with a variety of disabilities find the Card "friendly" to use. It would be undesirable for the Access Card to be physically indistinguishable from the variety of other cards that people will continue to have in their possession and equally undesirable for people with disabilities to be unable to recognise these cards and how they need to be inserted into readers without having to rely on third parties.

This is a simple problem to address and there are a variety of alternatives which might be considered (raised printing as with Braille; the use of large font printing; bevelled or chamfered corners, indentations, milling, lacunae etc). The Taskforce has been advised by card manufacturers with whom it has spoken that there are no technological barriers to this and that there are no major cost implications – although the latter point would need more express confirmation. The Taskforce does not wish to be prescriptive in this matter and believes that the Government should accept our Recommendation in principle and then consult widely with the Disability

Commissioner and the disability community about the precise nature of the features to be developed or used.

It is not desirable, in the view of the Taskforce for such disability-friendly cards to be issued only to people with disabilities – this may constitute further stigmatisation of such individuals – something which current public policy and anti-discrimination legislation seeks to minimise or eliminate.

The Taskforce recommends that:

> ***(9) a feature be built into the Access Card itself to render it as disability-friendly as possible and that all Access Cards be produced in this way.***

THE NAME ON THE CARD AND IN THE DATABASE

Although this is a matter more appropriately dealt with in detail as a consequence of consideration of Registration issues, the Taskforce nevertheless brings it forward here to request the Government to determine an important matter of principle at this stage.

It is accepted that the name of the cardholder needs to be displayed on the card itself. The issue is whether this name should be only the formal, legal name of the individual concerned (assuming this can be ascertained – which will not always be the case) or whether a "preferred" name is to be accepted on the card. Regardless of what decision is made about the name to be displayed on the card, there is clearly a requirement that the chip and/or the Secure Customer Registration Service (SCRS) contain the cardholder's legal name and, in addition, any other names by which they have been or are known.

The Taskforce recognises that there are legitimate reasons why people would want to have a name displayed on the card which might differ from their legal name. These include such matters as women having cards in their "maiden" names; the "Australianisation" of non-English names; the general use of preferred second or third given names (not uncommon among leading Australian politicians of all parties); the change of names in indigenous communities (for example with the adoption of skin names or name changes following familial deaths); the use of familiar diminutives; limitations on the physical capacity of the card to record names in full, and there are doubtless others which will emerge as Registration issues are considered. In the opinion of the Taskforce, taking a prescriptive attitude towards this issue by limiting consumer choice by legislative fiat would run the risk of substantially weakening public support for or acceptance of the Access Card.

Our consultations in the Northern Territory revealed to us that it is the standard practice in the Territory to issue Medicare cards in the name of all children, and that family cards are rarely issued. This is done for sound public policy purposes related largely to the cultural practices common in Indigenous communities. As a result of this practice name change issues (for example a child may not be given his/her formal name until some time after initial registration) have been further brought to our attention.

Constitutionally it appears that the determination of a person's name is a matter for the States and Territories under their relative births, deaths and marriages legislation. Generally these are quite flexible in allowing for changes of name, while at the same time establishing rules to prevent the adoption of names which are offensive or otherwise inappropriate. However they also usually recognise a principle which is set out (by way of example) in section 32 of the New South Wales *Births, Deaths and Marriages Registration Act 1995* which provides that the Act: "does not prevent a change of name by repute or usage."

A right of choice in this matter would also be consonant with our earlier Recommendation about the ownership of the Access Card and the right of customer choice.

The Taskforce recommends that:

> ***(10) the Government decide now that people will be entitled to have the choice of which name which they wish to have appear on the face of the Access Card provided that this choice is not misleading or deceptive as to the person's identity and that the chip and SCRS hold details of any other names by which the cardholder is, or has been known as well as their legal (i.e. birth certificate as issued or amended) name.***

PHOTOGRAPHS ON THE CARD AND IN THE DATABASE

Many submissions raised issues concerning the Government's proposal to include a photograph on the card and in the database.

The inclusion of a photograph on the face of the Access Card is a critical part of the Government's whole rationale for the introduction of this proposal to replace the multiplicity of specified cards and update the current Medicare card.

The Government has identified a number of essential arguments in favour of enhancing the new health and social services card by the addition of a photograph. These include:

- a photograph on the Access Card allows the easy identification of the cardholder at front line service delivery points in health and social services agencies, particularly Medicare and Centrelink. This is a direct benefit to consumers as it will speed up these transactions and enhance service delivery;
- a photograph on the Access Card will assist in the correct identification of cardholders when they undertake transactions with other services or agencies such as doctors, pharmacists and the providers of linked concessions (for example in areas of public transport);
- a photograph on the Access Card will allow the card to be used as a robust proof of identity document where the cardholder chooses to use it outside the health and social services environment, although there will be no compulsory requirement for it to be so used;

- a photograph on the Access Card, by providing for easy identification of cardholders, will be a major factor in preventing fraudulent health and social services transactions and/or detecting fraudulent activities.

However, the Taskforce recognises that the compilation of the first national photographic database of (virtually) all adult Australians, which will result from this policy decision, is a significant feature of the new Access Card arrangements. This is substantially more than an "incremental" or irrelevant change to current policy and practice. 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.

While demographic details stored on the SCRS may be thought to constitute a "thin" database, the addition of this national photographic database changes its nature qualitatively and fundamentally.

There are a number of countries that have national photographic databases. We are currently aware of a number of European nations such as Sweden, Germany, The Netherlands, Belgium and Switzerland that have national photographic databases. The Taskforce is aware that in some countries, such as Germany, access to the national photographic database is heavily restricted. However, with the exception of The Netherlands and Belgium, these databases appear not to contain biometric quality photographs and so cannot be used in the same way as is proposed for Australia. We also note that such a national biometric photographic database will be created in the United Kingdom if its national identity card programme is carried out fully, as proposed.

This raises significant policy issues which are discussed below. It needs to be recognised however, from the outset, that:

- Australians are increasingly likely to hold some form of photographic identification as a matter of course. This includes the holding of a passport, a photographic driver's licence, a photographic proof of age card, workplace based identification cards, and increasingly photographic credit and financial transaction cards. In some cases these photographic records are stored centrally by issuing authorities. In most cases they are not. There is currently no single, central, national government-controlled database of photographs (although passport photographs are stored centrally) derived from these
- the demographic details stored on the SCRS are to be limited to those items clearly specified depending upon final government decisions, but basically it will be: name; date of birth; address; dependents; Medicare, Centrelink or DVA status; card number and any such data as may be added voluntarily by the cardholder
- security protections will be implemented to prevent unauthorised access and to ensure that audit trails are maintained
- alternative models may be more privacy intrusive if they require storage on a multiplicity of existing agency databases

The Access Card has been designed with the inclusion of the photograph on the front as one of its key features and as the principal device by which recognition and validation of identity and prevention of fraud takes place.

Moreover, the KPMG Business Case relied heavily upon a card designed with this feature incorporated. It should be noted that the KPMG case for such an inclusion was not exhaustive and depended upon issues such as problems with the provision of readers to all access points (which could be particularly costly), especially as some of these access points would be in areas other than government offices. They would, for example be required in doctor's surgeries and pharmacies, and while the government has indicated already its intention to supply readers in these locations, there may be others which would need to be considered as the Access Card system matures.

Other arguments mounted in favour of displaying the photograph on the card relate to the possibility that in its absence, customers would be required to provide some other form of photo-identification to undertake transactions and that the granting and administration of related concessions would be more difficult because there would be no easy means of identifying the authorised concession holder personally.

The Taskforce needs to draw to attention that arguments in favour of including the photograph on the Access Card as they relate to the payment/administration of concessions are somewhat problematic until significant questions about how concessional status is to be identified have been resolved. In its discussion below about Concessions, the Taskforce endorses the current proposal which provides that concessional status will <u>not</u> be apparent on the face of the card but will become evident only when the card is inserted in an approved reader. We oppose suggestions that the card should show concessional status on its face other than those which relate to the replacement of the DVA gold card and the personal option which might be available to age pensioners (see page 53). For reasons which are obvious, DVA gold card status or optional choice of age pension identification do not carry the possibility of stigmatisation of concession holders in the way which might occur in relation to other concessional status identification.

It has been argued in some Submissions that the photograph should be contained not on the face of the card but in the chip itself so that it is not accessible by simply viewing the card but only when the card is inserted into an approved reader.

Chips can be divided into what are called "open" and "closed" zones. Data which is contained in the open zone is displayed whenever the card is inserted in an approved reader and can be read by anyone who has access to such a reader. Basic demographic data needed to administer health and social services payments needs to be accessible in this open zone.

Data in the closed zone is protected by a Personal Identification Number (PIN) and can be accessed only when the cardholder reveals the PIN details to another person reading or accessing the card. Such a closed zone would normally be used for storage of particularly sensitive data (such as emergency medical information) which does not need to be available for ordinary administrative purposes connected with authenticating and administering health and social services payments.

In analysing the proposal to store the photograph in the chip only, KPMG concluded that if the photograph were held in the open (i.e. non-PIN protected) zone of the card it might be vulnerable to illegal copying, whereas if it were held in the closed zone (i.e. PIN protected) problems could arise with customers needing to recall PINs for all transactions. KPMG concluded that such a proposition "is simply not a practical solution." (page 19)

On the other hand, if reliance is primarily upon card-holder identification simply by looking at the photograph on the card without recourse to checking the data in the chip, then where cards are copied/forged, this can become a means of by-passing the database and opening up, rather than closing down the opportunities for fraud. It would be naive, given the known history of the copying/forging of photographic driver's licences, to fail to acknowledge that such activity is a distinct possibility.

It has been argued in several submissions that there is no need for any photograph to be held in the chip or the database given that the identity of the cardholder will have been established at registration by use of the Document Verification Service. The Taskforce is not entirely persuaded by this line of argument since we see some value in there being a specified capacity to check photographs against an already captured image when it comes to detecting attempts at double registration, for card replacement requirements or to facilitate emergency payments.

Another frequently advanced position is that the use of the photograph on the front of the Card should be optional and left to the determination of the individual cardholder. This position has widespread support and is, we understand, the preferred position of the Office of the Privacy Commissioner in a strongly argued case presented to the Taskforce.

As with the argument for there being no photograph at all, the Taskforce is currently inclined to the view that the overall integrity of the system could be compromised in such an opt-in or opt-out arrangement, and that a decision needs to be on the basis of either no photograph or photographs for all except in exceptional circumstances. Its own position is to support the mandatory requirement for the Access Card to carry the photograph on the front.

[The Taskforce will consider the question of whether people with disabilities, people in palliative care, people too physically frail or incompetent to be photographed, or people with religious/cultural objections all of whom appear to be "low risk" in terms of threats to the integrity of the overall system should be exempted from being photographed, and if so, by what process of determination, as part of its forthcoming Registration Discussion Paper].

However, the case for a voluntary photograph has been made forcefully by a number of advocates, including the Privacy Commissioner, not all of whom are opposed to the overall Access Card project. This is perhaps a challenge for the technology experts to address, and the Taskforce invites them to do so as part of the further development of final architectural recommendations.

Any system of storage has the potential for serious misuse and abuse. People's privacy may be invaded by inappropriate access to their files and their personal

identity may be "stolen". Discussions between the Taskforce and several law enforcement agencies have drawn attention to the extent of current and possible future identity fraud. Recent reports have calculated this cost in Australia as being anywhere in the vicinity of $1.2 billion annually (cited in the KPMG Report) to $5 billion cited in a 2003 report from the Australian Institute of Criminology. [According to the United States Federal Trade Commission identity theft accounted for 43% of the 380,000 fraud complaints lodged in its Consumer Sentinel Database in 2002.]

The fraudulent capture of personal data, where these are used to create false identities or counterfeit cards, may have serious consequences for victims of such theft. Personal data must be captured in order to create false identities and/or false identity cards. This is done when personal data about a real person (for example their date of birth, address, mother's maiden name, dependents etc) is obtained and somehow attached to a photograph of another person or used in a situation where the checking of a photographic identity is not possible, such as in telephone or on-line transactions.

The victims of such fraud may subsequently find themselves, at least for a time, denied access to benefits, or that their benefits have been paid to other people. They may be subject to unnecessary investigation by law enforcement authorities who suspect them of fraud. They may face serious difficulties in (re-)establishing their own identities when these have been "stolen" or misappropriated by other people.

Our concerns in this area are well reflected in the recent House of Commons Report to which we have referred above. It says: "Security is a key aspect of the identity cards scheme. Having your credit card stolen is different from having your identity stolen: one can be rescinded and replaced, the other cannot." (para 131)

This means that the highest degree of priority must be given to ensuring that whatever arrangements are in place for the storage of all data, and wherever they are stored within the Access Card system, maximum security arrangements are incorporated for their protection. It should be remembered that the greatest threat to the integrity of the system comes not from external hackers, although their ability to compromise both the whole system and corrupt individual records cannot be underestimated, but from people within the system – those who have been trusted with access and betray that trust. The Taskforce is aware of the great efforts being undertaken by agencies to detect such improper behaviour and recognises that technologies may be available to prevent its occurrence in the first instance.

Nevertheless the greatest protection against such fraud derives from maintaining the absolute minimum of personal data genuinely required to administer any system which is collected/captured and kept on file in the first instance.

The full extent to which profiling (for example by race) and matching of photographs is possible, is not well enough understood – at least by the Taskforce, nor is the capacity of such a database to be used for medical diagnostic purposes. [The question here is whether a scan of the database can identify people whose facial biometrics reveal something about the state of their health, physical condition or disability.] The Taskforce is seeking advice on this matter.

The linkage of such photographs with other records, such as those derived from closed circuit television (CCTV) cameras was a matter drawn to the attention of the Taskforce. Such matching is certainly possible, although at this stage most CCTV recordings are of too low a quality of resolution to be so used. However, the Taskforce observed the procedures by which the NSW Police Service matches its database with photographs derived from other quality sources such as television footage and quality recordings from some fixed position cameras.

Questions have been raised about the quality as well as the method of capture of the photograph which has been selected (along with a digitised signature) as the biometric identification which is preferred, fingerprints and iris scans having been rejected. Again, this is a Government decision already made upon which the Taskforce offers no further comment. The issue of how such photographs are to be obtained in the first instance is yet another matter for consideration in the Registration phase of the Access Card project.

These concerns have given rise to a discussion about whether the photograph which is to be retained in the chip and/or the SCRS should be held in a "real" form or rather as a template, derived from the original photograph by application of an approved algorithm.

In essence the argument put to the Taskforce, is that holding a template enhances security and privacy. The template cannot be reconstructed into a real photograph, and thus there would be no value in seeking to steal or copy it.

On the other hand, the Taskforce is aware that there is a need for cards to be replaced when they are lost, stolen or damaged, and that such losses are not uncommon among the client groups of the participating Agencies. In such circumstances the process of replacement of an Access Card would be more easily facilitated both for users and government agencies were the replacement card able to be generated from the existing database rather than requiring the cardholder to represent themselves to be photographed again. It is not clear to the Taskforce whether it is proposed that every cardholder be re-photographed when their card expires or whether a new card will be issued automatically as is the case with the current Medicare card. If new photographs are taken another issue arises – will the old ones be retained, especially as they clearly have been superseded in use and functionality.

Information from the United Kingdom in this area appears unclear. Some sources suggest that the United Kingdom is proposing to store a full photograph in its national identity database while the House of Commons Committee Report to which reference was made earlier states: "The Government is proposing that the template be stored on the National Identity Register and on a chip in the identity card." (para 16)

One way in which this might be achieved would be for the SCRS itself to be segregated in such a way that the "real" photographs and the templates were held separately. Real photographs might need to be accessible for the purposes of the initial issue of the card and thereafter there would be general access to the template database for the purpose of checking or verifying identity, but additional steps would have to be taken to access the photographs themselves. This access would be separately logged and audit-trail marked and might be restricted to more senior

Officers of the participating agencies. Access might be restricted to specified circumstances (eg a fraud investigation, the need to resolve a false rejection by a card reader or card replacement). In our subsequent analysis of the SCRS we present a more comprehensive discussion about the more general segregation of the SCRS database into discrete entities.

The ability to check or match templates may depend upon the use of a particular software programme or a particular version of such a programme and it is undesirable for any scheme to be locked into dependence upon one vendor or technology. Systems improve over time. The algorithms themselves may become redundant or outdated as technologies are updated or replaced. The Taskforce was advised of the fact that the Department of Foreign Affairs and Trade had already been through the process of updating its photographic database systems associated with the new biometric passports on a number of occasions in a relatively short period of time.

In its advice to the Taskforce the Department and its Lead Advisors argued that the system should be based upon the retention of a real photograph in the SCRS because without it systems upgradeability would be compromised, the government would be locked into a particular vendor and their proprietary technology and that card reissue would be made unacceptably difficult.

Others put to us that the adoption of any such system of template storage does not automatically lock the Access Card programme into a specific vendor or technology. They claimed that there are several vendors and several technologies available, and that this being the case there is no need to be exclusively tied to any one.

In any event, consideration should be given to the storage of the photograph (wherever it is held) in a securely encrypted form. This encrypted photograph would be capable of being reversed engineered so as to generate a copy of the original photograph (for replacement purposes) only in a two step process which would require activity both by the database controller and by the individual concerned – analogous to the system used to manage safety deposit boxes in banks, although in this instance using a PIN system. The Taskforce recognises that this will not always be possible when fraud or law enforcement investigations are taking place, but absent such circumstances, the consent model should be the norm or preferred model.

Again, in response to this suggestion, the Department and its Lead Advisor argued that such a system would be problematic unless the government retained a "master key" to allow system upgrades and support the intervention of an authorised operator for an authorised purpose (e.g. to check potential false matches). If this were the case, the Lead Advisor questions whether or not any enhancement of privacy has been achieved, although there would certainly be an increase in complexity of usage. The Taskforce repeats the point made above in relation to fraud and law enforcement investigations : it recognises that there will be exceptions, but they should be minimised. If there is an additional complexity in the system in order to achieve better privacy protection, then that should be accepted as a price worth paying.

Many dangers are associated with the possible improper access to the photographic database. Any decisions to be made about the card must place a maximum degree of emphasis upon security and privacy protection.

Secondly, the Taskforce believes that public confidence and trust will be enhanced if it made clear that the photographic database cannot be hacked to secure people's personal images.

Thirdly, although cardholders who need to get replacement cards may be disadvantaged, there is some merit in making people more aware of the necessity to keeps their cards safe and not trivialise them because they believe the cards are easily replaceable. [Reducing the level of some 1.3 million replacements of the Medicare card each year would be highly desirable.]

Fourth, the Taskforce appreciates that reliance upon matching templates may result (for a variety of technical reasons) in a higher number of false positives (that is, failing to detect a double issue) – which may be avoided where a human assessor is able to look directly at both the cardholder and a terminal displayed real photo (as is done at passport control points).

Fifth, the Taskforce also understands that changes in appearance over time may be an issue here, especially when the images of young people are first captured and retained as they mature, and notes that reports by the London School of Economics in relation to the national identity card proposals in the United Kingdom have highlighted this point.

The Taskforce intends to advance more comprehensive arguments about questions related to card replacement in its forthcoming Registration Discussion Paper.

The Taskforce recognises that if card replacement is made more difficult, appropriate temporary provisions will need to be made to ensure that people are not denied benefits to which they have a legitimate entitlement. Such arrangements are already in place in many Agencies, and the Taskforce does not believe that this is an insuperable problem.

However the Taskforce is concerned about some arguments in favour of having such an "easy" system of card replacement as to put the integrity of the whole system at risk. The integrity of the Access Card programme relies upon the highest degree of reliability, consistent with its limited health and social services purposes, being built into the initial registration procedure where the biometric identifier is central. If at some later stage replacement cards can be issued without the necessity for secure biometric re-identification of the applicant for a replacement card the risk of harm to the whole system increases, as do the opportunities for fraud and theft. Ease of card replacement should not be allowed to occur to the point where it compromises the integrity of the system.

Finally, the Taskforce draws attention to the question of whether photographs of people who are deceased should be erased from the database. The whole question of what information needs to be retained and for how long, is in itself, complex and presumably subject to requirements under the *Archives Act* and related legislation. There are however major cultural questions, especially for Indigenous Australians, about the retention of the images, and indeed the names, of the deceased. These concerns should be acknowledged and responded to with sensitivity.

Related to this is the question of whether old photographic images are to be stored. It is clear that at regular intervals cardholders will need to be re-photographed. The Taskforce sees no valid reason whatsoever for the retention of a life-long catalogue of personal photographs of individuals in some central repository (even if it eventually be the Australian Archives). The Taskforce recommends that when replacement photographs are taken the previous photographs be destroyed.

On balance, the Taskforce sees great merit in considering the storage of the photograph as a template and not as a complete real photographic database. In the event that technical considerations and customer convenience arguments render this impractical we believe that there should be separate databases (which can both be contained within the SCRS if required) for the templates and the real photographs. In any event, photographs should be stored in a secure form.

The Taskforce accepts that it may be premature for the Government or itself to be absolutely definitive on this issue. In the final system design, the incremental privacy benefits of encryption, taking into account other security and privacy features need to be assessed against the possible degradation in system performance. We appreciate that encryption and decryption consumes system resources and is further dependent upon decisions which need to be made about the size/capacity of the chip and the design of readers. The Taskforce understands that final decisions about this aspect of the system architecture are yet to be made, and if this is the case, we trust that opportunities to adopt privacy enhancing solutions will be taken.

The Taskforce therefore recommends that:

> ***(11) the government note that there have been numerous submissions put to the Taskforce in support of the principle that the photograph on the face of the card should be voluntary rather than compulsory and that as a result there is some merit in the government revisiting this decision, bearing in mind that a determination needs to be made against the need to maximise the integrity of the system for personal identification of cardholders and noting the Taskforce's position on this issue which, at this stage, supports the use of a mandatory photograph on the card, with the destruction of old photographs when new ones are taken for card reissue or replacement.***
>
> ***(12) however, wherever the photograph is to be stored (on the card chip or in the SCRS) there is great merit in considering the storage of the photograph in the form of a template. In the event that it is decided to maintain a real photographic database, this should as far as practical be clearly separated from the template database and all photographs should be stored in a manner that ensures that rigorous controls are in place to prevent unauthorised access and improper disclosure.***

Before leaving this issue, the Taskforce notes that there are still questions associated with the whole process of facial recognition technology and that experience of its use overseas has been uneven, although the integrity and success of such systems appears to have improved significantly in recent years. The Taskforce is aware that some reports indicate that there may be issues which affect the success rates of biometric

matching, for example the varying success rates in matching males compared with females and among various racial groups. The Taskforce is seeking further advice on this issue. However, the question of achieving best outcomes in this regard should not be left exclusively to the registration phase of the card to sort out, they require earlier attention.

The Taskforce also considers it appropriate to report that in a number of consultations people expressed support for use of alternative biometric identifiers such as fingerprints rather than photographs, but that this matter has already been determined by a decision by Government which favours the use of photographs as the primary biometric identifier.

Consultations by the Taskforce with agencies such as the Attorney-General's Department and with private sector organisations such as the Biometrics Institute have persuaded us that it would be appropriate if some more detailed discussion was available in the public domain to facilitate debate around these issues. The Taskforce has observed directly some of the expertise developed already by State Police in facial recognition technologies, and notes that the CSIRO, the Customs Service and the Department of Foreign Affairs and Trade have also developed a number of relevant programmes.

The Taskforce has been privileged to be able to access information about the current developments in biometrics and the extent to which rates of biometric identification appear to be improving with the introduction of new technologies. It is aware of recent data which have been published, is familiar with some of the programmes in place in places such as Colorado and Florida in the United States and in some parts of Europe. It has also looked at standards and material published by the International Civil Aviation Organisation which is setting international benchmarks. Finally our attention has also been directed to the Biometrics Enrolment Trial conducted for the United Kingdom Passport Service.

The Taskforce is equally conscious of the fact that much of the integrity of the whole facial biometric recognition system will depend upon the conditions in which individuals are photographed in the first instance. There are also significant issues associated with the skills of the operators who will be taking these photographs. They will need to be appropriately trained and competent. These will be key issues for further exploration in our Registration Discussion Paper.

Knowledge of these issues needs to be in the public domain. If people are being asked to subject themselves to being photographed and those photographs are to be matched, checked or authenticated against something else using a particular technology, then it is the right of all consumers to know and be able to understand the technology being applied to them.

The Taskforce therefore recommends that:

> ***(13) the Government, as part of its Access Card project, commence a programme to publish information which allows a better understanding by the public of exactly what is involved in the technology of facial biometric recognition in relation to the Access Card programme.***

STORAGE

The multiplicity of legislative arrangements under which current health and social service data is collected and stored makes it difficult to determine the extent to which any of this personal data is eventually destroyed, or how the provisions of the *Archives Act* operate in this regard.

As a matter of principle, data should be held in any Access Card-related database for no longer than is required under other legislation which gave rise to its being required in the first instance. Ideally all such requirements should be uniform and the length of time during which personal data is held should be minimised.

The Taskforce does not regard it as an adequate response to indicate that there will simply be no change to existing practice or to refer people to obscure and unknown sections of archives legislation.

The Taskforce recommends that:

> ***(14) the Government make clear the current policy on the length of time and the public policy or legislative basis upon which data is held by participating Agencies, and the arrangements by which data is removed from the system.***

DIGITISED SIGNATURES

Many of the same issues captured in relation to the photograph arise when considering the other designated biometric – the digitised signature. [It is important to distinguish a digitised signature from a digital signature. The former is the representation of the handwritten signature of the individual in a digitised form on the card while the latter is a cryptographic means for providing non-repudiable, persistent proof of authenticity and integrity of an electronic transaction. (Rules for the latter are developed in the *Electronic Transactions Act* 1999.)]

Again, this digitised signature is proposed to appear on both the card itself and in the database. There are however a number of differences between the signature and the photograph for consideration. In the first instance, the participating Agencies already have some form of personal signature on file – they are pervasive on all manner of forms and applications already held. Nevertheless it must be recognised that the compilation of a national database of the signatures of virtually the whole population is a major initiative and one with serious implications in relation to potential fraud and misuse. This potential is minimised by keeping all unnecessary data off the database. Secondly while photographs do not change markedly over time, signatures do change and deteriorate – at different stages of life and due to the impact of disability or illness, signatures may vary considerably.

Checking of signatures can be difficult under these circumstances and comparisons can be hard to make. Digitised signatures are of little or no value in determining

crucial forensic questions (such as forgery) where such matters as the pressure on the paper left by a signature or the flow and regularity of the pen-strokes are critical. Everyday experience indicates to members of the Taskforce that the rejection of credit cards in bank or stores because a clerk/operator/teller has doubts about a signature on some document and that stored or displayed on a card, is a rare occurrence. Indeed even cursory checking is not always undertaken. The Taskforce was also informed in its consultations of the declining use of traditional signatures and their checking within the banking system itself. It should however be noted that the digitised signature on the card itself will not fade or deteriorate in the same way as signatures on existing cards tend to.

However there are questions which arise in relation to exactly how signatures are to be captured. These are more properly matters to be raised in the Registration Discussion Paper, but they include issues such as the marks made by people who are functionally illiterate or incapacitated (noting that procedures are already in place in some participating agencies which address this), who have difficulty writing in Latin script or whose signatures are difficult to capture within small boxes on forms or application documents.

It is hard to assess accurately the value of the digitised signature as a security device and the Taskforce is not aware of any robust argument which has been advanced for its inclusion, other than arguments of existing or common practice or tradition. In the absence of such an argument, the Taskforce prefers to work on the principle that it is advisable, wherever possible to minimise the amount of data displayed on the card in order to minimise risk, reduce the opportunities for fraud and eliminate the unauthorised capture or copying of personal data.

The Taskforce recommends that:

> ***(15) in line with its previous recommendation, further work be undertaken to assess the value and utility of including the digitised signature on the Access Card itself, noting that the Taskforce's preferred position is for it not to be included, and that***
>
> ***(16) in line with its previous recommendation and for the same reasons, if a digitised signature is to be included in the architecture of the Access Card then its storage in the database be stored in a manner that ensures that rigorous controls are in place to prevent unauthorised access and improper disclosure.***

More generally, the issue of the best security controls to be developed in relation to both the storage of photographs and signatures needs to be further developed on the basis of advice from the Lead Advisor to the project and its Chief Technology Architect. The Taskforce itself is not, at this stage, sufficiently confident to make recommendations about matters such as the security systems to be used.

However there is a clear opportunity here for improved security architecture to be introduced in relation to personal data held by government which will make a positive improvement over existing arrangements. Recent cases of inappropriate access to personal data in both Centrelink and the Child Support Agency have highlighted this problem. The Government has an opportunity to introduce technological responses

and solutions to enhance personal privacy and security, and should be giving priority to seeking these.

The Taskforce recognises that the Chief Technology Architect has a key role to play in providing the Government with expert advice about the overall design and operation of the Access Card. The Taskforce regards it as critical to its own work that it be able to consult with and receive advice from the Chief Technology Architect before it finalises all its recommendations regarding the design and operation of the Access Card system. Such a collaboration between two expert evaluators – one from a technical position and the other from a consumer and privacy position both enhances the quality of advice to government and ensures a greater transparency of the public policy making process.

The Taskforce recommends that:

> ***(17) a process be established in which the Taskforce, the Lead Advisor and the Chief Technology Architect consult to address the questions of what technology is both available and of best assurance to maximise the security of the card and the database in relation to the storage (in whatever form) of the photographs, signatures and other data to be collected from individuals. Further, that no final decisions on the security architecture be made without the advice of these parties.***

THE CARD NUMBER

Under the proposed Access Card programme each individual will be assigned a unique number. This number will be held in the chip and in the SCRS. It is also proposed that the number be displayed on the reverse of the card. At this stage the precise form of the number to be used has not been determined, although any such number may need to be compliant with ISO requirements.

This is a development which, in itself, raises some significant privacy issues. To all intents and purposes, the Access Card creates a form of unique personal identifier (UPI) which, for the first time, links several otherwise unrelated health and social services profiles of the one individual. It is axiomatic that in such a system as is proposed there will be such a number and that it will relate to one individual only, at least at any one time. The privacy question is how to minimise the impact of this creation of a UPI. In particular:

- how will the UPI continue to be restricted to use in the health and social services environment only
- how will this UPI be prevented from developing into a more comprehensive and ubiquitous personal identifier
- what structural or architectural features of the Access Card system can be designed to ensure that this function creep does not take place ?

In the case of existing Medicare cards, several family members may be listed on the one card and thus all be connected with the one number appearing on the face of that card. However there are separate unique identifying numbers for each person so listed

held in the Medicare system itself. In the Northern Territory where family Medicare cards are not issued each individual, including children, already have unique numbers issued and displayed on cards. Under the Access Card project there will also be children (i.e. persons under the age of 18) who will be eligible for personal Access Cards, although it is not clear whether or not they will also still appear as a dependent upon some other adult's card.

These are issues to which the Taskforce returns below.

The operation of the Access Card is such that the individual card number itself is not actually required for any transaction. Each participating Agency will retain its own agency-specific identifier which will be matched (via a translation table) against the common number held on the Access Card which would come to operate across several agencies.

The Taskforce is not aware that there are any circumstances in which the quoting of the Access Card number itself will be required, although there is a limited number of cases when it may facilitate making transactions with government easier. Indeed, we would be concerned if transactions were commenced or processed on the basis of the quotation of a number alone without additional steps being taken to verify the identity of the client or customer concerned. At present, as we understand it, even where the Customer Reference Number (CRN) is quoted in Centrelink call centre transactions, steps are taken by the Customer Service Officers (CSOs) to further verify the identity of the participating party. The Taskforce understands that this practice is current and will be retained in any operations undertaken in relation to the Access Card. A number on an Access Card should not be allowed to become a method of subverting this necessary cross-matching and identity confirmation.

The Taskforce notes however that Medicare Australia, Centrelink and the Department of Veterans' Affairs have expressed reservations about the elimination of the number from the face of the Access Card. Their arguments against its elimination have included a number of elements, which we understand to be as follows :

- their clients will be required to identify themselves by other means, perhaps involving multiple references and that this will make client interactions lengthier and more complicated and inconvenient for both Agencies and their customers
- some providers are required to quote an appropriate reference number in order to charge for and be reimbursed for services provided
- clients have difficulty in remembering numbers (where they are required) without these being easily visible
- an easily quoted number is required for on-line and call centre operations
- systems may fail and if they do, the processing of transactions will be compromised in the absence of a visible card number
- a visible number will facilitate customer's individual access to check their own records.

The Taskforce is not fully persuaded by these arguments, and notes that some are based on the assumption that existing business practices cannot or should not be changed to overcome any difficulties.

The majority of transactions (other than standard mail contacts) take place in environments when the Access Card will be physically presented and the relevant number required for the transaction (which will not be the Access Card number but the agency specific number) can be obtained through docking the card. In any event, the principal method of verification at this stage is by comparing the photograph on the card with the individual presenting it. Indeed, the proponents of the photograph have always presented this as their primary justification for its inclusion.

Where these transactions are on-line and the card cannot be verified by physical sighting of the individual concerned – the very purpose for which a photograph is being included – then reliance upon the number itself without other verification is problematic.

In relation to on-line customer management, the Taskforce believes that this purpose strengthens rather than weakens the case to take the number off the card. If a card is stolen or is being used fraudulently, then the fraudster will be in possession of the number. If this is then used to trigger an on-line interaction with a department or agency, the problem of fraud is increased not diminished. For on-line customer transactions, where the principal security feature of the card (namely the biometric photograph match) is not available, then reliance for authentication should be placed on a feature that cannot be ascertained from the face of the card – for example a date of birth, previous address, PIN or secret question.

The Taskforce is also conscious of the fact that all participating Agencies have existing policies and procedures in practice already to allow them to deal with people who present without their Medicare, Centrelink or DVA cards. We understand that such customers are not simply denied services until they produce their cards, but that they are assisted and accommodated at the time by other methods which involve identification, verification and authentication in the absence of any card. We presume that these services to customers will not be withdrawn after the issue of the Access Card.

The potential inconvenience of such verification needs to be weighed up carefully against the privacy and anti-fraud protection enhancements inherent in deleting the number from the face of the Access Card.

The Taskforce appreciates that the majority of actual contacts with customers is via the mail service and in these instances it is the name and up-to-date address which are the key elements in the transaction. Again, the utility of the number here is limited.

A further point was raised by some Agencies in relation to the "transition period" during 2008 to 2010 when they assert that not all agencies and points of delivery will be equipped with readers. Apart from hoping that this will not be the case and that planning will be sufficient to avoid such gaps in the system, the Taskforce again does not see this as a compelling argument that every card must, for all time thereafter (in effect), carry a number. There is an alternative – to issue the Access Card but to allow the continued use of old (Medicare, Centrelink etc) cards until such time as all service points are equipped with readers. The introduction of other smart card technologies has coped with this problem, either by having readers fully operational to meet new

systems or by allowing transitional arrangements for a limited period of time (as is done with the replacement of cash tolls by e-tags in a phased-in operation).

The Taskforce notes advice that the Department is confident that its own facilities will be equipped fully with the necessary readers at the start of the roll-out but cannot, be confident that this will be the case in relation to all private sector participants (eg doctors, pharmacies, private sector concession providers). In this instance the Taskforce is hopeful that the financial incentives which will exist for these service delivery points to be ready for business at the outset will work effectively. In any case it would not be an acceptable argument to make the enhancement of customer's privacy rights in any way dependent upon the failure of some private sector operators to be ready to comply with new requirements.

The allocation of this number, whether or not it is on the face of the card, of course raises a further matter of concern to privacy advocates – namely that this represents the compulsory creation for each Australian of a unique personal identifier (UPI) at least within the health and welfare sector. It is presumed, although it has not been made specific to date, that if an individual looses or has to have their card replaced, the new card would carry the same number as their previous card.

The Access Card number starts to develop at least some of the features of a UPI to the extent that it becomes the common number linking a set of unrelated separate transactions: for example Medicare payments, child support arrangements, organ donor status, concessional status or Centrelink benefits. UPIs are a crucial element of national identity card systems and the Taskforce draws attention, again, to the Government's clearly stated position that the Access Card is not, nor is it intended to become, a national identity card.

The question of UPIs has been a fraught one within the privacy debate for many years, and indeed some overseas countries specifically prohibit their creation for national identity purposes.

The Access Card number, which is a limited UPI confined to health and social services purposes should not be allowed to develop into, an expanded or comprehensive UPI for each Australian. One way of preventing this development is to ensure that access to the Access Card number itself is limited as far as possible and its details are revealed to as few people or institutions as possible – indeed only those with a real need to know.

As we have said, it was put to the Taskforce that the number should be retained on the card, in line with the original KPMG rationale and recommendations as a fundamental tool for on-line customer management and as a back-up for systems failures (eg broken readers, computer crashes etc). We were also urged to consider the fact that people are "used" to having numbers on cards such as the Medicare card.

The Taskforce questions the weight placed on the problem of potential system crashes. There are well known and available techniques and technologies to address this issue by the use of back-up systems which are in common use. The principles of Confidentiality-Integrity-Availability (CIA) are incorporated into back-up systems which keep the operation of major systems such as those used in internet banking, the

Department of Defence and others protected against such systems failures. In a system as large and complex as the one being developed to support the Access Card programme it is inconceivable to the Taskforce that fundamental design features intend to prevent an entire system collapse would not be in the process of active development and implementation. To design other parts of the programme on the basis that these may not work is, in the opinion of the Taskforce, not a suitable basis upon which to proceed.

As agencies develop voice recognition technology (as is already being pioneered in a number of them), this additional biometric will render the need for the number even more otiose.

Having considered the concerns of the participating agencies, the Taskforce would summarise its concerns about the inclusion of the number on the face of the card as being:

- the inclusion of the number on the card as well as in the chip and the SCRS adds to the potential for that number to develop into a more comprehensive UPI
- many people find the inclusion of the number on the face of the card to be objectionable in itself
- the potential for greater fraud and identity theft occurring where this number is improperly obtained or accessed, especially where it is used to trigger on-line transactions which cannot be verified by checking/matching the biometric photograph
- that the number itself serves no significant function to undertake a transaction since these actually require access to the individual Medicare, Centrelink or DVA number which themselves can be (and are regularly) accessed through identification means other than the Access Card number
- that there are more privacy enhancing alternatives available to establish and verify customer identity
- that all participating Agencies are already familiar with and regularly undertake the provision of services to people who fail to present the current cards which are in use.

Unless the Taskforce is seriously misinformed, it sees at best a weak rationale for the Access Card itself to display the number. It appears in this instance to serve no purpose, although of course the unique number must exist for the card to be issued and recognised. If the unique number must exist, then privacy interests would be better served if the card did not display the number, but that this was maintained only in the chip and the SCRS.

In fairness, the Taskforce recognises that for some individuals, the prospect of having a unique number assigned to them may be of less concern and they may, as a matter of personal choice decide to have this feature included on their card. The Taskforce appreciates that it addressed a similar question in relation to the optional nature of the photograph being included, but felt, on balance that it should be.

Indeed, it is the recommendation to include the photograph which has largely shaped our view that the inclusion of the number on the reverse of the card should be viewed with great caution.

It is open to the Government to approach this question by deciding that each cardholder should be entitled to make a choice as to whether the number is included or not on the reverse of the card.

If such a decision is made, then the choice available to each cardholder should be a genuine one. There should be no automatic "default" position either favouring or opposing the inclusion of the number. Each cardholder should be given a simple yes/no choice when completing their application/registration details for the initial issue of the Access Card. This is the current position in relation to matters such as enrolment on the Organ Donor Register which is offered for example to all applicants for drivers' licences who may elect to join the Register or not.

Individuals who believe that having a number on the Card will facilitate their dealings with government may elect to have the number printed on the Card. Such a procedure is recognised in relation to matters such as participating in the electronic health records system as provided under the New South Wales *Health Records Information and Privacy Act 2002*. This may be the more attractive option for individuals who have regular or extensive dealings with health, social service or veterans' agencies.

Those who believe that either this is not a major concern for them, or that they place a higher premium on the protection of their privacy may choose not to have the number so printed. This may be the more attractive option for individuals who have only limited health and social service dealings with government, such as people who currently hold only Medicare cards, or who make limited use of on-line or telephone services.

The Taskforce recommends that:

> ***(18) the Government notes the Taskforce's conclusion that there is a strong case for the number to be removed from the reverse of the card and reconsider the decision that the Access Card itself displays a card number, instead storing the number out of plain sight in the chip and the SCRS. In the alternative, the Government give consideration to making the inclusion of a unique number on the reverse of the card a matter of genuine choice for the individual cardholder.***

EXPIRY DATE ON THE CARD

It has been suggested in a number of Submissions that it would benefit consumers if the card itself indicated an expiry date. The Taskforce presumes that the Government will need to set at least a minimum period during which any one card would be in circulation: most documentation indicates a period of approximately seven years.

However, there may be some case for the random allocation of cards with a shorter (say five or six year) life, so that not every one of the 16 million cardholders will be

presenting for re-registration within the two-year period of 2015 to 2017 and every seven years thereafter.

After whatever time is allocated, the Access Card will need to be replaced, although details of this – for example, the necessity for a new photograph to be taken – have not yet been articulated. Clearly the process of re-registration will be complex and will involve many of the issues which will arise on the initial registration event.

In order to manage this process in a more effective fashion, the Government might well give some thought to a staggered re-registration period. This would be facilitated if cardholders knew the exact month and year in which they will be required to re-register.

At present there is no obvious way in which cardholders know this to be the case, although presumably participating Agencies would advise them either directly (by post) or when a transaction takes place near to the expiry date of the card.

It would be unfortunate if people found their cards had expired through some process of automatic cancellation or invalidity It should also be noted that although an expiry date has relevance to a particular individual it is not sensitive personal information in the same way as other information displayed or stored on the card and the SCRS.

The Taskforce recommends that:

> ***(19) consideration be given to listing the month and year of the Access Card expiry on the card itself.***

SCANNING / COPYING OF PROOF OF IDENTITY DOCUMENTS

It is proposed that when individuals present to be first issued with an Access Card they bring with them such POI documents as are specified and that copies be taken of those documents and those copied documents remain on file.

The Taskforce is not supportive of this proposal.

The Attorney-General's Department is currently in the process of developing its Document Verification System (DVS) which will allow a real time verification of basic identity documents including Australian passports, Australian-issued birth certificates, driver's licenses issued by State and Territory authorities and citizenship or other documents issued by the Department of Immigration and Multicultural Affairs. An Access Card will be approved for issue, in most circumstances only once POI has been established and a photograph and signature have been provided, although it is accepted that some cards may need to be issued prior to full verification if the DVS is not fully available and operational at the time. Hopefully the advent of the Access Card will spur the necessary sense of urgency in completing the DVS project.

However, it remains uncertain as to when the proposed DVS will become operational and whether it will be available to operate within the timetable proposed for the introduction of the Access Card. Similarly, doubts have been raised about the extent to which all relevant State and Territory records could be checked in an on-line environment. These concerns do not, however, detract from the key principle adopted by the Taskforce, namely that unnecessary amounts of personal data should not be maintained in government databases. Where such data does not need to be held (i.e. where State and Territory databases are adequate or when the DVS is fully operational) it should be deleted from the system.

The Taskforce has consulted with the Attorney-General's Department and understands their approach to identity verification issues within the framework of the National Identity Security Strategy (NISS). Quite properly, within this framework it aims to achieve a "gold standard" of identity verification which the Taskforce accepts is appropriate in relation to matters which go to the need to protect national security, achieve law enforcement goals; respond to the threats of terrorism and insure the highest integrity for documents such as the new biometric Australian passports.

However, as noted earlier, the Taskforce takes seriously the statements by the Government that the card is not intended to be a national identity card for national security purposes and that it is merely a replacement card for existing Medicare, social services and veterans' cards and other entitlement indicators. In this context it does not believe that the "gold standard" that may be required for national security purposes is necessarily appropriate for a card which is intended for use by recipients of health and social service benefits. In particular it notes that these recipients can include the most disadvantaged, marginalised and incompetent members of the community and that great care should be exercised in setting standards that could exclude such persons from receiving benefits.

Such an insistence would, inevitably, and with some justification, be perceived by the Australian community, as an attempt to establish a first base from which to build a national identity card system – despite government assurances to the contrary.

The Taskforce understands that the argument for the copying and retention of POI documentation relates to measures taken to detect and control fraud, and that such records are accessed by relevant Departments where there is some suspicion of illegal behaviour or identity fraud, or in cases where original documents are subsequently lost or destroyed. Such a procedure may, in some instances, also be required under statute. The Department asserts that there is what it sees as a strong case to retain POI documents used to establish identity to address subsequent identity inquiries and that such scanned documents may be required in some circumstances where verification via the DVS is not possible.

In many respects this argument about fraud detection relates overwhelmingly to the operations of Centrelink and the Taskforce has some sympathy with the point which is being advanced here. The point that needs to be borne in mind, however, is that the Access Card is not just replacing Centrelink-related cards, but all cards issued by Medicare and DVA. No substantial arguments have been put to us that there is a level of fraud in Medicare and DVA such as to require maintenance of such sensitive records for the life of a persons' interactions with the Agency – in the case of

Medicare this would mean effectively the whole of their life. To impose such an unnecessary privacy-threatening burden on (effectively) the entire Australian population to fix a problem (the exact dimensions of which are unstated) in Centrelink does not constitute sufficient justification for this procedure.

To date the Government has not indicated any special measures which might be put in place to secure the protection of this sensitive personal data if it is held in the SCRS. In the event that such data is retained, the Taskforce is of the opinion that special measures need to be in place to guard against its misuse – a matter revisited when we canvass the question of the segregation of different databases within the SCRS. The Taskforce is, of course, aware of the vast amounts of personal data and scanned documents already held on file in the various agencies: the more than 28 million personal files held by participating agencies and 275 kilometres of shelf space they occupy in Centrelink alone, has been referred to on a number of occasions in presentations by the Minister.

There is also no particular argument that retention of scanned documents is needed for the general reissue of the card when it expires. Leaving aside the question of taking a new photograph, there would be no need in any case to produce documents a second (third, fourth etc) time since the original card would not (presumably) have been issued unless these documents had been produced and validated in the first instance and since the whole rationale of the Access Card is to stop people having to "prove" their identity on more than one occasion.

The Taskforce however, does not regard the Government's arguments as sufficient justification for document retention, nor has it otherwise seen compelling arguments in support of the retention of copies of POI documents once verification – via the DVS or any other approved system – has taken place. On the contrary, the Taskforce believes that to retain this documentation would be not only an unwarranted intrusion into people's privacy, but more especially a significant risk to the security of the entire system.

Both the Government and individuals are concerned that steps must be taken to minimise the possibilities of fraud and identity theft (that is the unauthorised use of someone else's personal information for fraudulent purposes). The more information which is held on databases such as the SCRS [or indeed in related government files], the greater the "honey pot" effect attracting significant criminal and other elements to attempt to access that information for improper purposes. To give but one example: one of the most frequently used "security" devices in the finance sector is to ask people (especially in remote/telephone/on-line transactions) to give details of their mother's "maiden" names. This information is not generally available to third parties. However, if copies of birth certificates are held on file, then this data (together with information such as date and place of birth) will be accessible and obtainable – either through hacking, or more likely, via the improper activities of staff with access to such data. This information can be critical in the creation of false identities.

Any system is open to potential penetration. In a recent report the Australian National Audit Office has recommended the enhancement of security on the Australian Taxation Office portal after that portal was infiltrated recently by a "Trojan virus"

which copied several Tax File Numbers and Australian Business Numbers and published them on an overseas website.

Moreover, while current electronic systems used within agencies and departments make it possible to track who has accessed an electronically-held file and ensure that the access was authorised, where paper-based files are concerned, this is far less secure. Where photocopies of documents are simply attached to other existing paper records, details of who accessed them and for what purpose may be significantly more difficult to police.

The Taskforce has acknowledged that holding scanned copies of POI documents is a widespread and standard practice in some agencies at present. In our view it should not be and such a system should not be extended into the Access Card system. Although it is argued by the Department that very few people will have access to this information, no one can be certain how few this will be. Nor are there any guarantees that such systems are immune from external threat, potentially putting in the hands of undesirable elements almost all the data needed to create false identities. This new "honey pot" should not, in our opinion, be created in the first instance.

Constant repeat verification of original POI documentation is not required once an Access Card has been approved and the DVS called into use. Identity verification takes place through recognition of the biometric photograph or the matching of digitised signatures.

In its forthcoming Registration Discussion Paper, the Taskforce intends to raise the whole question of whether or not the production of POI documents is necessary in any event. There are alternative ways of establishing identity which may be less burdensome for consumers and more appropriate for certain sections of the Australian population. For example a "consent to check" authorisation may alleviate many of these concerns.

It is within this context that consideration needs to be given to the use of a Known Customer System. Such a system may have value in establishing identities for people with less than optimum POI documentation and may have value in pre-populating some aspects of the registration arrangements. It may also have some relevance where existing Departmental clients are well known and recognised, as is the case with most of the clients of the Department of Veterans' Affairs.

On the other hand such systems have the potential to simply restate (and almost validate) past errors, and pre-population may violate the information privacy principle related to the use of information for secondary purposes. The question of Known Customer Systems is a matter to be explored in greater detail in the Taskforce's forthcoming Registration Discussion Paper.

At the very least, if arguments can be mounted for temporary capture of copies of POI documentation – for example between the date of application for an Access Card and the approval/issue of the Card – then that capture should be genuinely temporary. This means having protocols in place for secure temporary retention and eventual destruction of retained POI documentation upon the actual issue of the Card, with

significant penalties attached to Agencies or specified Departmental Officials if this destruction fails to take place.

It is worth repeating that the purpose to be served here is one of verification not record keeping or data accumulation. It is a genuinely limited purpose and policies and practices should reflect this.

It is logically inconsistent for proponents of document retention to assert that such vast improvements are being made in the development and success of biometric facial recognition with success rates heading "north of 99%" and then say that documents must be retained to check because the system may fail.

The Taskforce recommends that:

> ***(20) POI documents should not be scanned, copied or kept on file once those POI documents have been verified.***

EMERGENCY MEDICAL AND OTHER DATA ON THE CARD

There has been general support in most of the Submissions for the government's proposal that individuals should be able to have certain emergency and medical data incorporated in the chip. There are clearly substantial benefits to be gained from having a robust, accurate and useful system of emergency notifications: inappropriate treatments and responses may be avoided and there may be quicker access to life-saving interventions.

However this is not without some problems arising, many of which have been referred to in submissions from medical, nursing, welfare, carers and pharmacy interests.

The first issue is that of data quality and verification. Emergency health data might include information about allergies, blood groups and the like. If this information is available to emergency and health workers, it is to be assumed that they might, in good faith, act upon it. This clearly has potentially life-saving or life-threatening consequences for the individuals concerned. Consequently there is a powerful and compelling argument that such data should not be listed in the chip without proper verification or authorisation by a medical practitioner. It should not be possible for any individual to list such data on their own initiative without verification – people might be (unintentionally) inaccurate in the information they provide or they might be badly motivated. Information may become outdated and again, potentially dangerous. The Taskforce believes that it would be relatively simple to devise a system by which appropriate verification (for example by medical practitioners on a standard form showing provider numbers and other relevant data) is provided before such information is incorporated. 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 Taskforce notes that in our consultations on this issue very complex medico-legal questions were raised but that it was made clear that it would be unrealistic to expect

medical personnel to rely upon any such data which had been entered on the card in an unverified system. We were also advised that in the very recent introduction of a similar health-related card in Lombardy (Italy) such a verification system was mandated.

The next issue that arises is the extent of such data that might be listed. For privacy reasons, the Taskforce does not favour allowing an open-ended approach to this issue so that what develops is a quasi-electronic health record established, effectively at random without appropriate standardisation or control. The Government should take steps to determine whether limits should be imposed on the extent of data stored, and what any such limits should be.

In this respect further advice should be sought about the desirability/practicality of links via the card to the national childhood immunisation register. The Taskforce notes that there is proposed to be a link to the Australian Organ Donor Register. In this respect there may also be requests for some linkage to registered Advanced Directives related to an individual's personal health treatments.

Thirdly, the listing of contacts of third parties, be they medical practitioners or friends/carers/family members to be contacted in the case of an emergency has privacy implications. There is clearly a benefit in being able to contact people in emergency situations and equally it is important to be able to identify if a person is either a carer for, or subject to the care of another person. On the other hand, people so designated may not have been made aware that they are the contact point, or, that as a result of activity on the part of another party, some personal data about themselves has been entered into the system. They may not have consented to be the contact point. A relative might have been designated who would become inappropriate in a change of circumstances (divorce, separation, family dispute) which might not have been corrected/amended by the cardholder at the time that the emergency contact was triggered. Medical practitioners might be inappropriately listed, for example in circumstances where the individual concerned had services provided by more than one such practitioner, without the knowledge of others, and with a consequence that differing treatments/prescriptions had been authorised. We are aware that this matter has been addressed in other contexts (eg the listing of contacts in the Australian passport) but it is still one needing to be approached in line with best privacy protection principles.

Fourth there is the question of how such emergency data should be accessed. It has been suggested that such data should be PIN protected, but this clearly faces problems in emergency situations where the cardholder is unable to state/recall the PIN in question. It may well be that hospitals or ambulances would be equipped with readers which over-ride PIN protection, but this may be a less than optimal situation. On the other hand it would be inadvisable for such data to be open to plain view by every other (non-medical) person with access to the card for health and social service purposes.

At present, Australia has a system called Medic Alert in which some 260,000 Australians are enrolled. Medic Alert provides bracelets or badges to its members who wear them on a constant basis in a way which alerts those providing medical and emergency treatment to call the Medic Alert number and be provided with

comprehensive health data about the subject person. Listing on the Medic Alert register follows a strict protocol which addresses all of the questions raised above about health status verification and the listing of emergency contact details.

It was put to the Taskforce in our consultations with the Medic Alert representatives that their system could be "contracted" by the Government to provide this service to all interested Australians through the Access Card scheme.

The Taskforce expresses no view on that proposal at this stage nor does it intend its comments to be seen as in any way being an endorsement of a particular medical alert or information system.

Currently, there is no way of knowing how many Australians would want to avail themselves of the facility of having such data incorporated into their Access Card, although the Taskforce believes that it would be considerably fewer than the 5.5 million or so who are on the Australian Organ Donor Register.

The Taskforce is also conscious of the fact that the Medic Alert system, built up over a period of some 35 years might be rendered less viable or indeed unviable by an open-ended approach to emergency health data listing via the Access Card.

There is clearly more work to be done on this issue and the interests of health consumers, the medical and related professions, the existing health alert systems and others need to be taken into account.

The Taskforce recommends that:

> ***(21) the Taskforce itself be authorised by the Government to consult further with representatives of all identified parties, to develop recommendations about the manner in which emergency health data should be incorporated within the Access Card programme and to subject any initial recommendations to extensive public exposure and comment before making final recommendations to the Government.***

The Taskforce draws attention, without making any recommendations, to the fact that a significant number of submissions have canvassed a greatly expanded role for the Access Card in terms of linking it with other health records. The Taskforce is aware of the work being undertaken across various agencies to progress a national system of linked electronic health records assisted by the work of the National E-Health Transition Authority (NEHTA). Any decision to link such records would be a significant departure from the stated purposes of the Access Card and would involve significant costs and delays in implementation. It would also need extensive public debate and support to be accepted.

As noted, the Taskforce makes no recommendations on this matter and raises it only to give an accurate reflection of the extent to which this question was raised in Submissions.

SYSTEMS / CHIP CAPACITY

It has been suggested to the Taskforce that one of the best ways in which "function creep" can be minimised or avoided is for the system itself to be designed in such a way as to impose physical constraints upon future expansions in scope.

This is a matter on which technical advice is clearly needed and is not within the capacity of the Taskforce to advise at this stage, although we understand that there must always be some spare capacity in the chip to allow for technological upgrades and security enhancements.

Our advice to date is that the most appropriate and readily available chip size would be 64 kilobytes (kb) and that such a chip would, given the currently proposed functions of the Access Card result in there being a spare capacity in the order of 25%.

Briefly stated, the proposition is that if the chip itself were of limited or restricted capacity, it would be more difficult for future functions to be loaded into it, thereby minimising or limiting the capacity for function creep.

On the other hand, to have no spare capacity in the chip might be unsound public policy, since future uses might be desirable (the method by which this desirability can be established or agreed upon is not being canvassed here) and a large investment of public money should not be made at this stage which precludes such enhanced activity in the future.

A limited capacity chip may be regarded as a protective and privacy-positive measure which would enhance public support. On the other hand it may be regarded as consumer-unfriendly in terms of preventing the development of some other function which has widespread public support or benefit.

The policy decision on this question is clearly one for Government, however that decision needs to be canvassed as part of the public debate. That debate, in turn, would be enhanced by having more information available about the technological issues which are raised in relation to this issue.

The Taskforce recommends that:

> ***(22) the advice which the Taskforce has received on this issue, in response to the suggestions made to it about chip capacity be made public.***

In our consultations the question was raised about whether or not the Access Card chip would be able to be read remotely, a feature available in many chip cards already in use. It is the understanding of the Taskforce that this is not the case, however this matter should be clarified by the government to avoid unnecessary concerns being raised.

EMERGENCY/DISASTER RELIEF FUNCTIONALITY

The initial information documents issued by the Office of the Access Card indicated that a possible use of the Access Card was "providing quicker and easier access to one-off disaster relief and emergency funds – faster access to payments," although no such function was canvassed in detail in the KPMG Business Case report.

The possible uses of such a function became apparent in the light of steps which needed to be undertaken to provide emergency assistance to Australians in the aftermath of the Cyclone Larry disaster.

Similar problems were addressed in the United States following Hurricane Katrina and the Taskforce is seeking some further information from one of its submitters about steps which were put in place to address these issues.

Similarly, those submissions which have expressed concern about this functionality of the Card have raised the question of what data might be captured by the banks, financial institutions or retail outlets where any such card-based benefits were redeemed. It is not possible for the Taskforce to be confident in its responses to all such questions at this stage, although it notes that there is no reason why such data should be captured. Current inter-bank arrangements to share ATMs rely on a simple yes/no validation of eligibility to withdraw stated amounts of funds.

However at this stage there is simply not enough information in the public domain for this question to be fully understood and debated. None of the material published so far by the Government explores all of the issues which need to be canvassed. The question of whether emergency/disaster relief payments are as far as the Government is prepared to go in this area needs clarification.

The Taskforce has been presented with some information about how such a system of emergency payments might be constructed, although issues about whether or not this would involve the use of further unique numbers (which could only be contained in a pre-issued magnetic stripe format) have left us in no position to evaluate the options which might be available at this stage.

The Taskforce therefore recommends that:

> ***(23) the proposed use of the Access Card for emergency/disaster relief purposes be clarified in a way which addresses the concerns raised to date in Submissions to the Taskforce.***

E-PURSE FUNCTIONALITY

The Taskforce notes that the Government's original position paper on the Access Card did not contemplate a developed e-purse functionality and there is no indication that this position has changed or indeed that funding for such a purpose has been approved. It is our understanding that the Minister has clearly ruled out this proposed use for the Access Card in its current iteration.

The Taskforce has noted a significant number of suggestions which contemplate the development of an e-purse functionality, especially about how the use of the Access Card could be expanded in relation to financial transactions (as well as those related to health-linked issues). However the Taskforce sees these as something of a distraction from the principal issue – namely how to ensure the effective primary uses of the Access Card as articulated by the Government.

The role of the Taskforce is to bring to the attention of the Government that such suggestions have been made and have attracted wide support in a number of quarters.

CONCESSIONS

No subject has been more difficult to understand and come to grips with than the way in which concessions operate arising from the issuing of initial health and social services cards by the Commonwealth. As a result of the possession of a Commonwealth card of some sort, an individual may become eligible for concessions issued by the Commonwealth, State, Territory and Local Governments as well as by private sector providers. Such concessions range from those involving massive expenditure, such as pharmaceutical benefits and public transport concessions, to smaller amounts such as local government rebates and even those whose value cannot be calculated such as discounted haircuts and entry to cinemas. It has not proved particularly easy to even establish a comprehensive list of what concessions are available, especially through the private sector, nor the value of those concessions.

It is clear that bringing some coherence into the operation of this multiplicity of concessions would be one of the areas of the operation of an Access Card which would have maximum benefit for consumers.

Aspects of the concessional system have been reported upon by the Australian National Audit Office (*Administration of Health Care Cards* No. 54/2004-5) and the House of Representatives Standing Committee on Family and Community Affairs (*Concessions – who benefits?*, October 1997). These and other reports have raised problems with the concessional system, for example reporting that some 25 percent of all health care cards are cancelled by Centrelink before they expire. State and Territory Government have expressed concerns that there is significant "leakage" in their revenues because of an inability to monitor, with sufficient accuracy, which concession holders continue to be eligible for the concessions which they provide.

The current Access Card project envisages a form of "flag" identification which would not appear on the face of the Card but would be held in the SCRS and in the chip and which would indicate to the participating Agencies, when the card was read, that the individual concerned was eligible for a particular concession. Such a system would obviously fulfil the requirements and needs of those Participating Agencies, and they could make alterations in the SCRS to ensure that concessional status was kept up to date whenever an actual transaction took place. They would not however, as the Taskforce understands it, be able to do this on-line or remotely without the active involvement of the individual concerned. The Taskforce supports a flag system

for concessional identification and would be strongly opposed to having concessional status made obvious on the face of the card, either by colour-coding or other markings, unless this was specifically requested by the cardholder, as such identification and possible stigmatisation of concession holders would not be acceptable.

The Taskforce appreciates that Veterans' are often very proud of their DVA "gold" cards and indeed wish people to be able to identify them as holding special concessions which are related to their defence force service. It has always been envisaged by the Taskforce that "gold" Access Cards would be issued to eligible Veterans to replace their gold DVA cards. Similarly, people who become eligible for aged-based concessions (Age Pensions) may like to have an Access Card which clearly indicates this. The Taskforce is supportive of this right of choice but reiterates its opposition to any involuntary concessional status identification.

It is clear that a great deal more work needs to be done in this area. As concessions involve all levels of government, resolution of these complex issues will undoubtedly be the subject of extensive negotiations. The Taskforce considers that concession providers and the general public need to be presented with options that are convenient to consumers, low cost and privacy protective or enhancing.

The Taskforce recommends that:

(24) a priority be given to resolving the issues arising in relation to the operation of the concessions system and that the options or decisions be explored in a way which allows informed public input to the final decision making process.

THE SECURE CUSTOMER REGISTRATION SERVICE (SCRS): THE ARCHITECTURE OF THE CENTRAL DATABASE

Even among those Submissions which reject the idea of the Access Card outright "as a matter of principle", the real issue is always the database. When analysed, most of the opposition to the proposal revolves around the idea that a central database is to be created, and it is the existence of this database which poses unacceptable threats to our privacy or security.

As we identified in our initial Discussion Paper, few areas will be of greater interest to or a source of concern in the community than the question of who will be able to access the personal data held about them, through the database which is connected to the operations of the new Access Card.

As a result, there will be few areas related to the Access Card and its database (the Secure Customer Registration Service) in which it will be more important for the Government to state with absolute clarity, consistent with the Information Privacy Principles, exactly:

- how the system will detect unauthorised access or misuse
- what penalties will be imposed for unauthorised access or misuse
- how the SCRS will be kept secure especially from misuse, from hackers and from unauthorised usage and personnel
- whether and how individuals will be easily able to check their own data held in the SCRS [To facilitate this, the Taskforce believes that it would be desirable for participating agency offices to have a stand-alone card reader accessible to any cardholder to dock their own card in order to check the data on it.]
- whether individuals will have the right to know who has accessed their data, and if so, how will they be able to find out
- whether individuals will have a right of redress in the event of the unauthorised access, use or disclosure of their personal data
- who will monitor this whole system and will they be sufficiently independent of government
- how the system will ensure that data is accurate when it is entered for the first time and what procedures will be in place to ensure that the data is kept up to date and accurate.

It would be unrealistic not to recognise that law enforcement and national security services may have cause to seek authorised access to the SCRS including its biometric components. However, if there is to be public support for and trust in the new Access Card system, then those rights of access must be clearly stated pursuant to statute and subject to independent oversight. This is clearly already the case as far as federal law enforcement and national security services are concerned – they operate under their respective statutes and they are subject to independent monitoring. The Taskforce understands that there are no proposals being considered by the Government to vary any of the procedures which are now in place to deal with any such requests that may be made.

It has been put to the Taskforce that as a database the SCRS as proposed is relatively "thin" (leaving aside the issue of the photographs) in comparison with databases already held in the various agencies, and this is undoubtedly true. Nevertheless even quite anodyne information may have major security and privacy dimensions. For example identification of the address of a person seeking to escape from acts or threats of domestic violence may be fatal if leaked into the wrong hands – indeed there have been such examples. No data is valueless. As such it demands the highest level of security and protection.

The Taskforce thus approaches its recommendations on the SCRS conscious of the need to both achieve the government's stated objectives and at the same time address the concerns that have been expressed about having a new database which is seen as a potential threat to personal privacy.

Accepting that it will be necessary to hold some form of photograph for security (to prevent double issue) purposes or to facilitate replacement of cards, it could be argued that this could be done via what might be described as a system in which such photographs are held in a form which has robust access controls. This, it has been suggested may involve some authority completely unrelated to the health and social services system and whose data could – by statute – be immune from any other form of access. This is akin to the holding of data in what might be described as an "escrow" system. The Office of the Privacy Commissioner has been suggested to be such an appropriate place.

On the other hand, as we have already noted, it might be possible or desirable to store the real photographs, templates, basic demographic data, personally entered emergency data and (if these are retained) scanned POI data in separate databases, although they might all be held in the SCRS, but in different sections of the database with different rules for access.

This concept of separate sections (silos) of the SCRS could ensure that in areas where access is needed for management, maintenance or upgrading purposes these are kept separate from those sections which hold actual personal data. Government officers involved in system management do not need to have access to personal data for this purpose.

There could then be different levels of access into the SCRS on a "need to know basis". This would mean that a front office staff member may be able to access only the demographic database when uploading data on change of address where it might

not be necessary to access the photograph at the same time (the card having been validated via the template). Access to other parts of the SCRS could be restricted in a way which allows such access to take place only with the express consent of the cardholder via a PIN or secret question system.

Such a structure would, in the opinion of the Taskforce go some way to addressing the concerns of individuals about large numbers of agency staff being able to access their complete files or records when such complete access is neither warranted not desirable.

Such systems seek to address some of the threats to privacy which arise from either external hackers or from insider-misuse. They may prevent "function creep". They have the capacity to enhance trust once people recognise that control of their own data is more securely in their hands and that encryption systems reduce the risk of fraud or theft.

By enhancing public confidence in the security of personal identity, it is claimed that e-commerce will be promoted, and that the current low levels (2-4%) of on-line government health and social services transactions will be enhanced.

The Taskforce does not see itself as able to evaluate all the technical and technological issues that such a proposition gives rise to although it has seen examples of smart cards with a number of separately locked functions held on the one card.

The Government has advised that external experts from the Defence Signals Directorate (DSD), the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) and accredited, independent, specialist information technology assessors from the private sector will provide guidance on all security aspects associated with the Access Card system. This will include security principles, policies, standards, guidelines, procedures and architectural and technical specifications, which, we understand, the DSD will independently review and accredit prior to the system going live. DSD will also undertake "red team" testing to attack the system from both an internal and external point of view in order to expose any potential security weaknesses. ASIO will independently review all physical aspects of the security implementation. The Government has also advised that there will be stringent access controls, logging and auditing of access to the SCRS.

Accepting this advice, and acknowledging the considerable level of discussions which have already taken place between the Taskforce , the Department and the Lead Advisor, the Taskforce still sees some attractiveness in an alternative approach proposed particularly in relation to the idea that the SCRS, (if that model is adopted), should be divided into a number of discrete databases accessed in different circumstances, on either a "need to know" or a customer consent model.

The Taskforce appreciates that the whole area of smart card technology is advancing rapidly. The extent to which the Access Card becomes more "card-centric" rather than "database-centric" is an important area of debate which should be resolved sooner rather than later.

Finally, the Taskforce notes that there has been no discussion about where the SCRS (and any presumably separate, back-up system) will be located in a physical sense. Clearly this is a significant security issue which we presume will be addressed at an appropriate time.

The Taskforce therefore recommends that:

> ***(25) further work be undertaken involving all relevant parties, including the Taskforce, seeking the advice of external experts, (DSD, ASIO, AFP, etc) to evaluate the proposed security architecture of the Access Card to ensure that it optimises security, privacy and consumer convenience.***

A COMMERCIAL ALTERNATIVE TO THE SCRS

Perhaps the most radical and far-reaching suggestion put to the Taskforce by an interested commercial party was that the central database, the SCRS, was itself not necessary for the system to still operate effectively. It was argued that reliance should instead be placed on storing information in the chip rather than in the SCRS. It was argued that a principle of data security – never store the same data in two different places – should be recognised and that a decision should be made which in effect replaces the one central database, under the control of the government, with 16 million mini-databases each in the control of the individual who holds the chip-enhanced card in their possession.

This proposal would see all relevant data held in the chip and not replicated in the SCRS. It would see data updated by updating the chip. Thus for example when a chip was updated for a change of address or any other basic demographic, then when the card was used in another Agency, the updated data from the chip would flow into the database of the second agency and update its records. Such an update could take place at any time when a cardholder interacted with any of the participating agencies.

The Taskforce was informed that the technology was available from a variety of sources to build the card in such a way that it would release data from the chip only to an authorised recipient and that the Government could use a technological solution to ensure that data flows were restricted in this way.

The proponent of this system outlined it, as stated above, as replacing the Government's massive and potentially at risk, single database with 16 million far less risky databases held and controlled by individuals – usable only in authorised places/transactions – updated on-line with escrow backup systems. In short, it's all about the chip not the database. They would characterise the system as one built upon smart cards and dumb databases rather than the other way round. They also assert that such functionality and operability for smart cards, interacting remotely with databases is well-established technology.

However, there is then the question of whether such an approach runs the risk of locking the Access Card system into one vendor or proprietary model. Secondly there is the question of whether this is a proven technology or in effect an untried one and whether its possible adoption would expose the Government to unacceptable financial and other risks.

A further question arises as to whether such an approach, if adopted, would make it more difficult for the whole system to be upgraded and for the technology to be refreshed as better algorithms are developed.

As noted above, the Taskforce does not regard itself as being in any position to evaluate this proposal but does not dismiss it as an idea not worthy of further consideration and as a matter of discussion with the newly appointed Chief Technology Architect and the Lead Advisor.

CONCLUSION

The Taskforce believes that within the time constraints under which it is seeking to operate, this Paper raises the questions which need to be addressed at this stage of the programme's development. It realises that many of the questions raised by the Taskforce require the input of people or organisations with greater expertise that the Taskforce possesses and it looks forward to active dialogue with them.

It acknowledges that the process of calling for public submissions and undertaking broad-based consultations has been a most valuable exercise and it trusts that this Report reflects accurately the purport of those submissions and consultations.

It also appreciates that many of the questions deferred from consideration at this stage, to consideration in its forthcoming Registration Discussion Paper will be just as vital to the success of the Access Card system as are these current issues of design and architecture. It is thus looking forward to a similar process of submission and consultation informing that exercise.

The Taskforce is strongly of the view that whatever decisions are made finally by the Government about the architecture of the Access Card and the Recommendations in this Report, there is a critical need for the Government to undertake a comprehensive programme of public education about the nature of the Access Card and its ramifications. This is necessary in order to ensure full public understanding and to engender the public trust which will be needed if the Access Card is to fulfil its intended purposes.

In line with assurances given about the openness and transparency of this process, and in line with best practice –

The Taskforce recommends that:

(26) after consideration by the Minister, this Report be made public.

Professor Allan Fels AO
Professor Chris Puplick AM
Mr John T D Wood

Access Card Consumer and Privacy Taskforce
25 September 2006

CONSULTATIONS

Below is a list of bodies with which consultations have been undertaken to date:

Aboriginal Medical Service – Danila Dilba, Northern Territory
Aboriginal Medical Services Alliance – Northern Territory
Access Card No Way Campaign
Aged and Community Services Australia
Attorney Generals' Department
Australia Medic Alert Foundation
Australian Association of Practice Managers
Australian Bankers Association
Australian Bureau of Statistics
Australian Chamber of Commerce and Industry
Australian Consumers' Association
Australian Consumers' Federation
Australian Council of Social Services
Australian Customs Service – SmartGate Facility
Australian Divisions of General Practice
Australian Electoral Commission
Australian Electrical and Electronic Manufacturers' Association
Australian Federal Police
Australian Federation of AIDS Organisations
Australian Government Information Management Office
Australian Injecting and Illicit Drug Users' League
Australian Law Reform Commission
Australian Medical Association
Australian Nursing Federation
Australian Privacy Foundation
Australian Sex Workers Association (Scarlet Alliance)
Australian Taxation Office
Australian Transaction Reports and Analysis Centre
Australian-French Association for Science and Technology
Biometrics Institute
Booz Allen Hamilton
BQT Solutions
Cancer Council
Cancer Voices
Carers Australia

Carers WA
Central Land Council, Northern Territory
Centrelink
Child Support Agency
Civil Liberties ACT
Clayton Utz & Pacific Privacy Consulting
Community Housing Coalition of WA
Computer Sciences Corporation
Consumers' Health Forum
Council on the Ageing (over 50's)
Cystic Fibrosis Western Australia
Department for Community Development (WA)
Department of Employment and Workplace Relations
Department of Finance and Administration – Gateway Review
Department of Foreign Affairs and Trade
Department of Health and Ageing
Department of Human Services
Department of Immigration and Multicultural Affairs
Department of Veterans' Affairs
EDS
Electronic Frontiers Australia
Ethnic Communities Council of Western Australia
Families Australia
Family Medicine Research Centre
Federation of Ethnic Communities Councils of Australia
Financial Services Consumer Policy Centre
Giesecke & Devrient
Global Platform
Health Consumers' Council (WA)
HealthConnect NT
Human Rights and Disabilities Commissioner
Institute of Clinical Excellence
Internet Industry Association
Isolated Children's Parents' Association of Australia
Joint Committee of Public Accounts and Audit
JPMorgan
KPMG
Learning Centre Link (WA)
Liberty Victoria

London School of Economics
Mater Hospital (Brisbane)
Medicare Australia
Mental Health Law Centre (WA)
Microsoft
Motor Vehicle Registry, Northern Territory
National Archives of Australia
National Association of People Living with HIV/AIDS Australia
National Children's and Youth's Law Centre
National Council for Single Mothers and their Children
National Farmers' Federation
National Institute of Standards and Technology
National Rural Health Alliance
National Welfare Rights Network
Northern Land Council, Northern Territory
Northern Territory Police
Northern Territory Registrar of Births, Deaths and Marriages
NSW Council for Civil Liberties
NSW Police
NSW Registrar of Births, Deaths and Marriages
Office of the Privacy Commissioner (OPC)
OPC - Privacy Advisory Committee
OPC - Health Leaders Forum
Orima Research
PA Consulting
Pharmacy Guild of Australia
Public Interest Advocacy Centre
Queensland Transport
Regional Women's Advisory Council
Returned Services League
Royal Australian College of General Practitioners
Senator Bob Brown
Senator Natasha Stott-Despoja
Smartcard Alliance (USA)
SmartHealth Solutions
Telstra
Trust Centre
Unisys
United Kingdom Home Office

Victorian Health Services Commissioner
Victorian Privacy Commissioner
Victorian Transport Ticketing Authority
Vietnam Veterans' Counselling Service
WA AIDS Council
Western Australian Council of Social Service
Youth Affairs Council of WA

SUBMISSIONS

Below is a list of submissions that have been received by the Task Force to date:

Prof G Greenleaf, Faculty of Law, University of New South Wales

Australia Medic Alert Foundation

P Fullerton

Rural Clinical School, Faculty of Medicine, University of NSW

B Bowes

Dr R Hosking

Australian Privacy Foundation

J P Foster

Prof W J Caelli AO

Association of Independent Retirees - Bundaberg and District Branch.

Health Consumers' Council

Department of Premier and Cabinet (TAS)

N Phillips

Office of the Health Services Commissioner

Access card No Way Campaign

Australian Health Care Association Ebsworth and Ebsworth

Preventative Health National Research Flagship, CSIRO / Queensland Health E-Health Research Centre

Australian Federation of AIDS Organisations

NSW Council of Civil Liberties

Lawyers Reform Association

Privacy Commissioner (VIC)

Ethnic Communities' Council of Victoria

Commonwealth Bank of Australia

Health Issues Centre - La Trobe University

Australian Bankers' Association

Public Interest Advocacy Centre

Abacus Australia Mutuals

Australian Medical Association

Council of Social Service of NSW

Computer Sciences Australia

Australian Computer Society

Electronic Frontiers Australia

Australian Electrical and Electronic Manufacturers' Association

Carers Australia

Consumers' Health Forum of Australia
Civil Liberties Australia (ACT)
Australian Council for Civil Liberties
Investment and Financial Services Association
A/Prof G Ross
M Yonwin
Australian Society of Archivists
Office of the Privacy Commissioner
Department of Health and Ageing
Biometrics Institute
Australian Nursing Foundation
Westpac Banking Corporation
Pharmacy Guild of Australia
Royal Society for the Blind
JPMorgan
Royal Australian College of General Practitioners
Australian Divisions of General Practice
Australian Chamber of Commerce and Industry
Federation of Ethnic Communities' Councils of Australia
Australian Association of Practice Managers
Dying with Dignity Victoria
National Women's Advisory Council
Unisys Asia Pacific
Datacard South Pacific
Lockstep Consulting
Development Systems
Oberthur Card Systems
Keycorp
Sony Australia
Placard
Medseed
Asia Pacific Smartcard Forum
Visa International
KelTec Industries
Information Integrity Solutions
B Fels
L Tavener
Presidian Legal Publications
J Melville

N Ashworth
D S Lucas
T Worthington
J Ekegren
A Beeton
R Andrew
PricewaterhouseCoopers Australia
Martin
M Moore
A Jones
A Kent
N McIntyre
T Trevor
Telstra Corp
E Montgomery
M Sakara
D Dwyer
A Waters
L Whitefeather
Legacy Co-ordinating Council
C Hingley
P Bubb
M Stanley
D E Boesel
N Taugge
J Whittaker
C Beavis
M Thomas
E Knight
Z Casper
B Blackburn