Australian
Privacy
Foundation

# What we do (and don't) know about the proposed 'Access Card'

## *An Information Paper with questions for the Government, and answers for the public*

***Version 1***

13 July 2006

This Information Paper is intended to provide a comprehensive resource for anyone interested in:

- facts and figures about the so-called 'Access Card' proposal
- what is clear – and what is unclear – about the proposal
- what some of the implications of the proposal might be, and
- what questions should be asked of the Government to find out more

This Information Paper will be revised regularly as we obtain more information about what is proposed under the auspices of the so-called 'Access Card' proposal.

Updated versions will be made available at www.privacy.org.au.

## Contents

# The top 10 questions for July

1. What information about me and my family will be on the card, on the chip, and on the national population database?

2. Who will be able to access what information from the card's chip?

3. Who will be able to access what information from the national population database?

4. How will centralising all our personal information in the one place make it more secure from hackers, organised criminals or corrupt or lazy staff?

5. If this card is about improving customer service and enabling things like optional recording of emergency health information, why does it need to be compulsory?

6. How will the proposed biometric facial recognition technology work if there is a case of identity theft?

7. Why is this project being introduced before either the review on the adequacy of the national privacy laws, or the national smartcard framework and strategy, is finished?

8. How can the Government say this will work as a national, uniform, multi-purpose "photo proof of ID", but then say it is not a national ID card?

9. If the Government won't release the privacy advice it commissioned on this proposal, and won't release the details on how it expects this proposal to achieve the alleged financial savings for Australians, how can Australians assess for themselves whether the social, financial and privacy costs are worth the benefits?

10. Will the Government conduct a referendum to test whether Australians really want this national ID card?

# Introduction to this Information Paper

The Australian Privacy Foundation was founded in 1987, by individuals opposed to the national ID card then proposed, the 'Australia Card'.

Our objectives include protecting the privacy rights of Australians, by means of research, awareness, education and campaigns; and focussing public attention on emerging issues and technologies that pose a threat to the freedom and privacy of Australians.

To that end, we have developed this Information Paper about the current proposed national ID card, the so-called 'Access Card'.

Despite being billed as the biggest IT project ever to be undertaken in Australia, few details are yet known about how the system would work. The KPMG-prepared 'business case' was heavily censored before its release; the Privacy Impact Assessment commissioned by the Government has not been released at all. Most of what we know is from scattered press releases, media reports and answers given to inquiring Senators in Parliament.

From what we do know so far, we believe the proposal, as it stands today, will result in a national ID card system, impacting significantly and deeply on every Australian's life.

Our aim with this Information Paper is therefore to highlight the many questions that must be asked of – and answered by - the Australian Government, so that Australians can fully appreciate all the proposal's implications – costs, benefits, privacy impacts, and social impacts. Only then can we have an informed debate about whether or not this proposal should proceed.

We believe that every Australian has the right to consistently ask these questions of the Government. These are also questions that we hope the media, the Australian Privacy Commissioners, and the Parliamentary Opposition will take up and pursue.

However in particular, we believe that the principal and urgent task of the Consumer and Privacy Taskforce, headed by Professor Allen Fels, is to get the answers to these questions, and make them available to the public.

The Australian Privacy Foundation will continue to ask these questions until we get answers.

---

### About the Australian Privacy Foundation

The Australian Privacy Foundation is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about us see www.privacy.org.au

## *Glossary of terms*

| | |
|---|---|
| Budget Estimates | Commonwealth of Australia, Senate, Finance and Public Administration Legislation Committee, Budget Estimates, Canberra, Proof Committee Hansard, 25 May 2006.<br>Evidence was given by Mr Geoff Leeper, Acting Secretary, Department of Human Services, and Mr Graham Bashford, Acting Head, Office of Access Card. |
| CSA | the Child Support Agency, part of the Department of Human Services |
| DHS | Department of Human Services – incorporating Medicare Australia, Centrelink, the Child Support Agency, Australian Hearing, CRS Australia (Commonwealth Rehabilitation Service), and Health Services Australia |
| DVA | Department of Veterans' Affairs |
| KPMG Report | Department of Human Services, *Health and Social Services Smart Card Initiative*, Volume 1: Business Case, KPMG, February 2006, *Public Extract* released June 2006 |
| SCRS | Secure Customer Registration Service – the name of the proposed national population database to underpin the Card system |
| Taskforce Discussion Paper | Access Card Consumer and Privacy Taskforce, *Discussion Paper No. 1: The Australian Government Health and Social Services Access Card*, 15 June 2006 |

# Project rationale and claims

## *Project objectives*

Q: What is the primary objective of the so-called 'Access Card' proposal?

> The project is described as intending to use "smart card technology to improve the access to - and delivery of - health and social services benefits for Australians" (Office of Access Card website, http://www.humanservices.gov.au/access/index.htm ).
>
> The KPMG-prepared 'business case' states: "The primary intent of the initiative of which a new card is part, is to improve service delivery by improving upfront access to services and entitlements, making the system more efficient, easier to use and less vulnerable to fraud" (KPMG Report, p.3).
>
> When questioned in the Senate, officials suggested that "customer convenience" was the main driving force, not "savings" (Budget Estimates, p.88).
>
> Likewise the Consumer and Privacy Taskforce describes the Government's argument for the proposal as because "it benefits consumers and it improves Government service delivery" (Taskforce Discussion Paper, p.9).
>
> Yet the only quantified benefits in the 'business case' prepared for the Government related to projected savings by reducing welfare fraud, and KPMG recommended that the system be made compulsory, because it would not otherwise create a "sound value proposition" (KPMG Report, p.10).
>
> Even the Consumer and Privacy Taskforce says that the "reduction or elimination" of losses caused by fraud (whether provider fraud or recipient fraud) "is a key secondary driver for the implementation of the access card" (Taskforce Discussion Paper, p.29).

Q: What evidence is there that Australians currently lack any 'access' to health benefits or social services because of the absence of a smartcard?

Q: If this project is about improving "access to - and delivery of - health and social services benefits", why didn't the Government first ask recipients of those benefits how their customer experience might best be improved?

Q: How can the Government say that delivery of services will be 'improved' if *no* services will be delivered to people without a so-called access card from 2010?

> In a tortured piece of rhetoric, the KPMG business case says that the proposal will improve "service access by ensuring that consumers are able to authenticate who they are and demonstrate their entitlement to services, thereby strengthening the integrity of program outlays" – meaning the 'proof of identity' bar will be set higher, so some people will lose their access to benefits (KPMG Report, p.3).
>
> So the Government is saying that included under the umbrella objective of "improving customer service" is actually reducing the number of people claiming benefits, which saves the Government money. This is not about improving the quality or efficiency of customer service at the level of the individual – and for people without the card, there will be no service at all.

Q: Is this proposal really only about 'access' to the services or benefits provided to people through DHS and DVA?

No, it's also about revenue-raising for the DHS, financial savings for both DHS and DVA, and creating an all-purpose ID card for both government and business to use.

One of the DHS agencies that doesn't get mentioned much in the Government's literature on the proposal is the Child Support Agency. While the Minister has announced several other initiatives (such as video surveillance and data-matching with Centrelink) to crack down on what he terms "deadbeat dads" who avoid paying child support, he has been remarkably quiet on how this proposal for a national ID card, and a national population register listing family relationships and dependents, will affect those perhaps unwilling 'clients' of the CSA.

Non-custodial parents don't receive "services" or "benefits" from the CSA – they provide money to it. We're not saying that's a bad thing – but the Government should be more honest about its description of this proposal than suggesting it is only about 'access' to 'benefits'.

Q: If the Card is supposed to improve the delivery of services to the 'customers' of DHS and DVA, why would the Government need to bother making it compulsory – won't the customer benefits be enough to make people want one?

When a trial of the Medicare smartcard was rolled out in Tasmania on an optional basis, only 1% of the population took it up. The Government has now cancelled the project, without formally evaluating why there was such a low rate of take-up. Anecdotal evidence suggests people could not see the benefits to themselves, or found it too expensive to enrol, as they needed to obtain original copies of their birth certificates (Budget Estimates, p.125).

When a Government needs to prop up a new method of 'service delivery' by making it compulsory, you know the idea is already in trouble.

Making the Card and registration compulsory is of course not about delivering benefits to the individual – it is about creating a national ID Card and national population database. It is intended to make the Government's life easier, not ours.

## *Claims about improving customer service*

Q: How will individual Australians ('customers' or 'consumers') actually benefit?

The Consumer and Privacy Taskforce has said the Government needs to address "the question of how exactly consumers will benefit" from the proposal (Taskforce Discussion Paper, p.18).

Q: What claims are made about improving customer service?

The KPMG Report (p.10) suggests that the improvements to customer service delivery that will arise from the so-called access card are:

- replacing 17 cards with one
- enabling people to only register once for all DHS / DVA services, and only have to notify once of each change of address or other details
- enabling online service delivery (as a user authentication device)
- enabling 'on-the-spot' confirmation of concession status (including PSB safety net status)

- could be used as an 'electronic purse', so customers could withdraw Centrelink payments (one-off disaster relief entitlements, or other "specified funds") from an ATM or EFTPOS machine
- could contain optional additional information such as allergies, drug alerts, chronic diseases, organ donor status, immunisation records, emergency contact details and health service provider details
- can be used as an all-purpose 'proof of identity' card

It should be noted that only four of these alleged benefits actually relate to customer service transactions with DHS or DVA – the other three relate to transactions conducted with third parties, from pharmacists, to other government agencies, to banks, to any business that wants to see photo ID.

## Replacing 17 cards

Q: What are the 17 cards to be replaced?

"the current Medicare card, Medicare Australia Organ Donor Registration card, Medicare Reciprocal Health Care Agreement card, PBS Safety Net Entitlement card, PBS Concession Card, Cleft Lip and Palate card, Centrelink Pensioner Concession card, Centrelink Healthcare card, Centrelink Foster Child Care card, Centrelink Low Income Healthcare card, Centrelink Commonwealth Seniors card, Centrelink Electronic Benefit Transfer, DVA Gold Repatriation Health card, DVA White Repatriation Health card, DVA Repatriation Pharmaceutical Benefits card, War Widow/Widow's Transport Concession card and the Office of Hearing Services voucher" (*Fact Sheet (Supporting Information)*, DHS website)

Q: Why is making everyone get a new card more 'convenient' or 'efficient'?

A major selling point for the Government is that 17 cards will be replaced with one. Yet its own business case warns the Government: "It is important not to overstate the problems of multiple cards" (KPMG Report, p.5).

Q: How big a problem is this: how many people have all 17 cards now? 16? 15? …

The Government hasn't said, but we suspect no one person has 10 of the cards to be replaced, let alone anything close to 17.

Q: How many people hold more than 2 or 3 of these 17 cards?

The 1.9 million aged pensioners in Australia "are highly likely to have three to four cards" (KPMG Report, p.5).

Q: At any given time or in any given year, how many adults are in receipt of benefits from DHS and/or DVA (i.e. relating to the 16 cards) *other than* Medicare?

About half the population: 8 million adults, or 12 million Australians including children, receive some form of social security payment, not counting Medicare, in any given year (KPMG Report, p.11).

About 22% of people aged over 15 have social security payments as their principal source of income (e.g. the aged pension), while the remaining 28% receive payments on top of their principal income (e.g. the baby bonus) (KPMG Report, p.11).

Q: At any given time or in any given year, what % of adults hold (or are listed on) *only* a Medicare card (i.e. do not hold any of the other 16 cards)?

Roughly half the adult population receive no social security payment, and so are only customers, or potential customers, of Medicare.

While around 3.5 million people do not access any Medicare service in a twelve month period, it is "highly likely most people in this group (have) a current Medicare card", because "Medicare is a universal system" (KPMG Report, p.62).

Q: Why does the 50% of the population which receives no social security payment need this card at all?

The Government's business case says the so-called access card "will bring several attractive benefits" to the 8 million adults who receive social security payments (KPMG Report, p.11).

However the report struggles to explain how the remaining 50% will benefit at all, let alone justify why the card needs to be compulsory:

- "they will only have to register for their health and social services once" – this ignores the fact that we are talking about people who don't access social services, only health benefits, and are already registered for those health benefits, with an existing Medicare card
- "they will be able to have vital personal information such as their emergency contact information in a safe accessible environment" – this flimsy use of one of the *optional* features of the proposal, to justify why the proposal should be *compulsory* for this half of the population, ignores both the fact that "a safe accessible environment" is an oxymoron, and that people could achieve the same objective with a laminated piece of paper in their wallets, instead of a massive government database
- "they will have a more valuable POI to gain access to other services" – this of course has nothing to do with improving customer service related to health or social security benefits, and suggests a level of demand for an all-purpose national ID card that we contend does not exist

## Single customer record

Q: How will a single customer record benefit me when I change my address?

A major selling point for the Government is that when you move address, or change your circumstances, you will only need to notify one agency, instead of many (*Family case study*, DHS website).

"When your details change, for example if you move house, you'll be able to update your information through a portal online at home or by visiting one Government office—whatever is most convenient. The card will then be updated to reflect the change when you next put it into a Government terminal" (Joe Hockey speech to the AMA National Conference, 27 May 2006).

However DHS has already developed a project called "single-sign-on", which is due to launch in September 2006. This will be a website that provides a single point of access to Centrelink, Medicare and the Child Support Agency, allowing customers to send a 'change of address' or 'change of circumstance' notification to all three agencies at once ("Smartcard not so clever: fraudster", *Sydney Morning Herald*, 16 May 2006).

Q: If a single customer sign-on as about to be launched (without a smartcard) to enable single 'change of address' or 'change of circumstance' notifications, why do we need the so-called access card as well?

Q: If a single customer record is the best benefit for individual customers of the various agencies, why not just implement this feature on an optional basis, without needing a smartcard?

Q: How else might a single customer record make life easier?

> The Government has claimed that the proposal for a single customer record (held in the SCRS) will "make it easier to do business with Government by such improvements as pre-populating certain forms (i.e. sending out forms with some of the consumer's personal details already included on them)" (Taskforce Discussion Paper, p.9).
>
> However this practice of mailing out pre-printed forms to customers, used for some years by financial institutions (e.g. when encouraging customers to sign up for more credit cards, insurance policies, etc) has been criticised as posing increased risks of identity theft through mail interceptions. Stealing mail from letter boxes, and using the details obtained to steal the recipient's identity in order to open new accounts or access the funds of legitimate account holders, was a key method used by a recently-discovered organised crime ring ("Vigilant teller unmasks major identity theft ring", *Sydney Morning Herald*, 12 July 2006).

Q: What is the estimated risk of increasing identity theft if this proposal for increasing 'customer convenience' by pre-populating forms is introduced?

## Faster service delivery

Q: What type of 'efficiency benefits' are likely to come about under this proposal?

> The Government claims that around 580,000 people each year queue at a Centrelink office, only to find they have the wrong documents they need to claim a benefit (*Fact Sheet (Financial Case)*, DHS website). The implication is that the so-called access card will 'solve' this problem.
>
> The Government also claims that there will be time savings of 3.5 minutes for each of the 2.9 million face-to-face interactions each year with customers presenting new claims at a Medicare or Centrelink office. However these time savings have been calculated based on Centrelink staff estimates, not on the basis of demonstrated experience in the application of smartcard technologies elsewhere (KPMG Report, p.5).

Q: What % of the 580,000 people who have the wrong documents relates to people who present with the wrong documents about their identity - as opposed to people who present with the wrong documents about eligibility such as level of income or assets?

Q: What estimate has been made of the number of people who would still forget to bring their so-called access card, and thus have a wasted trip to Centrelink?

Q: Will the so-called access card mean people can reduce their visits or phone calls to Centrelink?

Probably not: “while a person will need to only register once and prove their identity once, they will need to continually provide relevant asset, income and family composition information as per the existing policies of DHS agencies”; and the “majority of service settings will be face-to-face” (KPMG Report, pp.3, 20).

## Enabling new modes of service delivery

Q: Will the ‘efficiency benefits’ include enabling online service delivery?

That is one of the proposed benefits.

To date only 2% of DHS customers use online channels (KPMG Report, p.6). One of the problems with both online and telephone interactions is the need to provide authentication. Centrelink’s current system of “secret questions and answers” (SQA) do not provide the two-factor authentication and non-repudiation now required under the Australian Government’s Authentication Framework (KPMG Report, p.6).

However it is anticipated that even with the card, the “majority of service settings will be face-to-face” (KPMG Report, p.20). Online service delivery using a smartcard depends on the user having a smartcard reader attached to their PC – which will only slowly become commonplace.

Q: Will the ‘efficiency benefits’ include the ability to get instant Medicare rebates at the doctor’s office?

The Minister Joe Hockey has met with the big four banks to discuss using their transaction systems to process Medicare transactions such as bulk billing refunds and concession entitlement refunds using EFTPOS (“Banks set to reap rewards of smartcard”, *Australian Financial Review*, 2 June 2006, p.3).

He’s also promised doctors “a new claiming system that will deliver improved patient and doctor convenience … with the introduction of the access card there is now a compelling argument for the expenditure necessary to make electronic claiming work” (Joe Hockey speech to the AMA National Conference, 27 May 2006).

However the Australian Government Department of Health & Ageing has also said that its “Broadband for Health” program is partly about enabling “swipe and go” technology, so that patients can swipe both their Medicare card and their bank card at the doctor’s office, to receive instant Medicare rebates and thus eliminate the need to visit a Medicare Australia shop front (Presentation by Tam Shepherd, E-health branch of the Department of Health & Ageing, to the CHF E-health national information workshop, Canberra, 29 May 2006).

Q: If there is a pre-existing commitment and program to delivering on-the-spot Medicare refunds at the point of health service, why is this so-called access card necessary to deliver the same ‘efficiency’ benefit?

Q: Will the so-called access card be used to change welfare payments so that they carry restrictions, such as only allowing the purchase of groceries or payment of rent and utilities bills?

DHS has said that the card could potentially be used in the future to allow welfare payments to carry restrictions, such as only allowing the purchase of groceries or direct debiting rent or utilities bills, but not to be used for cigarettes or alcohol (“Commercial access on the cards”, *The Australian*, 12 May 2006).

## Obtaining concession entitlements

Q: How will the card improve people's ability to obtain their concession entitlements?

## Obtaining disaster relief

Q: How will emergency/disaster relief be 'delivered' through the so-called access card?

> It has been suggested that "Centrelink … will be able to download small amounts of money onto the card which the customer can go and recover from an ATM" (Budget Estimates, p.74).
>
> Questions remain about why downloading stored value to an ID card will be any better than directly depositing money into the bank accounts of existing Centrelink customers – if ATMs and EFTPOS machines are not operating due to power failures caused by a flood or cyclone, a smartcard will be no better than a bank card.

Q: What does the Government mean by 'disaster relief'?

> It has been suggested that instead of cash payments to people affected by natural disasters, such as Cyclone Larry, 'stored value' would instead be 'downloaded' onto your Access Card, if you lived in the affected area. That value could then be used to draw cash from an ATM or EFTPOS.
>
> It has also been suggested that the stored value could be used to purchase groceries at major retailers such as Coles and Woolworths – but not cigarettes or alcohol ("Commercial access on the cards", *The Australian*, 12 May 2006).

Q: Is this feature genuinely part of the proposal?

> Although this component was one of the features that added up to a "sound value proposition" in the view of KPMG, evidence from Departmental officials suggested a lack of certainty about whether this feature might work at all, let alone clarity about *how* it would work. One official said: "there is not necessarily an expression of intent. We are just noting that the technology supports its use as an electronic wallet, should government choose to do that" (Budget Estimates, p.75).

Q: How many people receive disaster relief each year?

Q: How many people who receive disaster relief are not already customers of DHS or DVS?

## Additional optional features

Q: What 'optional' features are being promised?

> The Government has said that card-holders will be able to choose optional information to store on the card, such as "emergency contact details, allergies, health alerts, chronic illnesses, immunisation information or organ donor status" (*Fact Sheet (Technology)*, DHS website).

While this information may be useful in an emergency, it can also include very sensitive health information and other personal information. This poses privacy and data security risks, which are unlikely to be strictly controlled – the Government will likely just say, "if you don't like it, don't use this feature".

Q: What research has been done into the efficacy or utility of storing this information on a chip inside a 'secure' card which needs a reader to access it, as opposed to say a laminated piece of paper kept in one's wallet?

It would appear the Government has not given consideration to low-tech means of achieving the same objective, such as a separate laminated card kept in your wallet and never used except in emergencies.

Q: If this health information is stored in the 'public' area of the chip, who else will be able to see it?

Q: Will sensitive health information, emergency contacts etc, stored in the 'public' area of the chip, be vulnerable to unauthorised capture and use?

Yes. KPMG has noted that "anything stored in the 'public zone' is potentially vulnerable to being captured electronically without the permission of cardholders" (KPMG Report, p.19).

Q: What research has been done into whether emergency personnel such as paramedics or accident & emergency staff would actually read and rely on medical information presented on a smartcard, as opposed to simply treating a patient based on presenting symptoms?

## *Claims about welfare fraud and identity fraud*

### Welfare fraud

Q: What % of the estimated up to $3 billion in financial savings relates to reducing "welfare fraud"?

The Government has claimed that "KPMG has found that the introduction of the access card would lead to substantial cost savings from improved efficiencies, and a reduction in identity fraud, abuse of concession entitlements and errors. KPMG estimate the savings could be as much as $3 billion over ten years" (*Fact Sheet (Financial Case)*, DHS website).

The KPMG Report itself says that "fraud savings could range from at least $1.6 billion to $3 billion over a ten year period" (KPMG Report, p.12). However details are not provided of where those savings will come from.

Q: Is the $3 billion estimate about all welfare-fraud reduction proposals, or just the smartcard?

The language in the KPMG Report is a little hazy on this point. It doesn't actually make the direct claim that this proposal will generate $1.6 to $3 billion in financial savings for the Government.

So is not clear whether the claimed $1.6 to $3 billion relates only to this so-called access card initiative, or to the sum total of savings that could be achieved if all fraud was resolved: "KPMG have provided ongoing advice to the Australian Government that

fraud savings could range from at least $1.6 billion to $3 billion over a ten year period" (KPMG Report, p.12).

However Minister Joe Hockey answered "Yes" when asked directly: "I wonder whether the minister can confirm that the $3 billion over 10 years is specifically and directly related to the introduction of the smartcard" (Parliamentary debate on *Appropriation Bill (No. 1) 2006-2007*, 19 June 2006).

Q: What % of the health and welfare budget is affected by welfare fraud?

The projected maximum potential savings of $3 billion is "a relatively marginal trim", representing only 0.3 to 0.4% of the total annual outlays (Budget Estimates, p.62).

Q: What % of welfare fraud across the DHS and DVA agencies relates to Medicare, versus the other benefit agencies?

Rather than Medicare, "the bulk of the savings would come from Centrelink customers" (Budget Estimates, p.62).

Q: Given the bulk of identified welfare fraud comes from Centrelink, what % of the fraud relates to the deliberate supply of incorrect information about identity (identity fraud), as opposed to incorrect information about eligibility (e.g. level of income or assets)?

Q: Are the estimated financial savings from reducing welfare fraud only in relation to identity fraud (as opposed to eligibility fraud)?

The KPMG Report appears to collapse both categories into its estimates; for example it claims that the biggest gains are likely to include the "reduction of fraudulent claims for benefits from Centrelink through non-disclosure of changed personal circumstances" (p.12).

This suggests to us that either the financial savings estimates are wrong, or the proposed ID card and/or SCRS is intended to work in conjunction with other, intrusive methods to also address eligibility fraud.

## Likely impact on identity fraud

Q: How will adding photographs impact on welfare fraud?

The Government has stated that "The access card will contain a high quality digital photograph, also referred to as a biometric photograph. … A biometric photograph can be translated into a mathematical algorithm and used to test for similarity of appearance against the biometric photographs of other people…." (*Fact Sheet (Technology)*, DHS website)

(Note however that the algorithm is not the set of numbers derived from a photograph, it is the method for doing the reduction. The proper term for the reduced biometric dataset is a "template".)

Q: What % of the estimated financial savings in reducing identity-based welfare fraud are expected to be realised by DHS / DVA staff checking that the photograph on the so-called access card matches the person presenting before them – either manually (a visual check) or automatically (a computerised check against the card and/or database)?

Q: How might the so-called access card impact on the wider problem of identity fraud and identity theft in Australia?

The KPMG Report predicts a "an initial sharp reduction in fraud and other leakage when the new system is implemented" (KPMG Report, p.12). However the report provides no analysis beyond that point.

The Attorney General has stated that a national ID card "could increase the risk of fraud because only one document would need to be counterfeited to establish identity". (Philip Ruddock, 29 June 2005, Australian Smart Cards Summit). Furthermore the National Identity Security Strategy, announced in May 2005, is based on a recognition that our current system of multiple identity documents should be strengthened, not replaced, in order to tackle identity fraud and the crimes it supports.

Indeed the Australian Taxation Office has said the so-called access card will cause a ***rise*** in identity theft – as creating a new fake identity becomes more difficult, organised criminals will instead steal real identities. Indeed identity theft may even become easier to perpetrate with the introduction of the so-called access card - because when you reduce a person's identity to a number, it is easier to steal. Identity theft is of more concern to the Tax Office than identity fraud, accounting for 74% of tax-related identity crime ("Identity theft to take on new life: ATO", *Australian Financial Review*, 24 May 2006, p.53).

Australia's leading criminologist has also warned that instead of using fake birth certificates, methods such as bribery, corruption and hacking would instead increasingly be used to obtain fraudulent or stolen identities (Presentation by Dr Russell Smith, Principal Criminologist, Australian Institute of Criminology, Biometrics Institute Conference, 9 June 2006).

Q: What is the estimated dollar value of the new identity fraud and identity theft likely to be generated by this project?

## Alternatives to tackling welfare fraud

Q: How else could welfare fraud be tackled?

A number of projects have been implemented or announced recently relating to reducing fraud relating to Centrelink benefits, including:

- a voice authorisation service
- anti-fraud computer systems ($5.1 million in capital announced in the 2006 budget)
- data-matching with private sector employers, the Department of Health and Ageing, and land title registries ($282.3 million was allocated over five years in the 2006 budget)
- pilot programs to examine further data-matching with the ATO, Child Support Agency and Medicare ($5.7 million with respect to the ATO, and $4.8 million with respect to data-matching with DHS agencies, was announced in the 2006 budget), and
- the Document Verification Service ($28.3 million announced in the 2006 budget). (Ben Woodhead, "Data matching strikes out fraud", *Australian Financial Review*, 11 May 2006, p.47; and "Budget 06-07" lift out, *Australian Financial Review*, 10 May 2006, p.B18)

KPMG has also identified that between $75 million and $150 million annually is being overpaid by Centrelink to people who are recorded in their own records as dead (KPMG Report, p.7).

Q: Given these many existing and new projects to tackle welfare fraud, why is the so-called access card needed at all?

Q: Why shouldn't these other, more targeted initiatives be implemented and evaluated prior to introducing a far more intrusive and expensive project with the same objectives?

Q: In its examination of the business case for the so-called access card, did KPMG consider the likely impact of these other initiatives?

Q: What risk has been identified that the so-called access card might not achieve the claimed $3 billion in financial savings because they will have already been achieved by these other initiatives?

## Impact on data-linking and data-matching between Government agencies

Q: What % of the estimated up to $3 billion in financial savings for the Government relates to "improved efficiencies" in relation to data-linking programs?

We don't know. The Government has just claimed that "KPMG has found that the introduction of the access card would lead to substantial cost savings from improved efficiencies, and a reduction in identity fraud, abuse of concession entitlements and errors. KPMG estimate the savings could be as much as $3 billion over ten years" (*Fact Sheet (Financial Case)*, DHS website).

However the business case prepared for the Government hints at the greater use of data-linking, and secondary use of customer information, than exists now. Unfortunately the detail has been censored.

Under the heading "more efficient services", the KPMG Report (p.11) states: "The registration process and common record of demographic information will provide agencies with better data to undertake analysis of both financial outlays and program outcomes. Sentence deleted for Cabinet in confidence reasons".

Q: How can some parts of the KPMG document be "cabinet-in-confidence", but not all of it?

## Abuse of concession entitlements

Q: What is the 'value' of a concession card?

The value to the recipient of a pensioner concession card is about $1,400 (Budget Estimates, p.61).

Q: What does 'abuse of concession entitlements' refer to?

When a person is no longer entitled to a concession (because their circumstances change), but they continue to use their existing concession card until the date of its expiry, as printed on the face of their concession card.

The Australian National Audit Office has estimated that 25% of concession entitlements are cancelled by Centrelink prior to the expiry date on the concession card (KPMG Report, p.7).

Q: What amount of money each year is lost through 'abuse of concession entitlements'?

This hasn't been quantified by the Government.

To the Commonwealth Government, the most significant risk area would appear to be with respect to PBS medicines. We would expect most demand for subsidised or free medicines would come from the elderly or people with disabilities – i.e. people on the aged pension or disability pension.

However short of winning a lottery, these people's circumstances are fairly static, and so their concession status is unlikely to change much over time, compared with say a person on unemployment benefits or a sole parent's pension.

It is therefore not clear that the 'abuse of concession entitlements' by people whose concession status has been cancelled, but who continue to use a card to claim discounts, is affecting Commonwealth government outlays to a significant degree.

In any case, not all the concession discounts claimed are against the Commonwealth Government – for example, pensioner discounts are available on public transport, council rates, utility bills, movie tickets, etc. So only some of any savings from reducing abuse of concession entitlements will flow back to the Commonwealth Government.

Q: How is concession status checked now?

From the rhetoric around the benefits of the so-called Access Card, you would think concession status wasn't already capable of being checked in real-time. But it is.

According to Centrelink's website, Centrelink's Confirmation eServices (CCeS) are internet-based facilities used by organisations to confirm a Centrelink or DVA customer's current entitlement status to receive a concession.

Presumably businesses make a judgment call, based on the size of the benefit or discount being claimed, as to whether or not they take the time to check the currency of the person's concession status.

Q: How is a smartcard any improvement on CCeS, the current online method to check concession status?

Q: How will a smartcard fix the problem of "abuse of concession entitlements"?

A smartcard can have information about concession status stored by way of a 'flag' on the chip in the card. For example, reading the chip might yield results such as: "unemployment benefits: no; aged pension: yes; PBS safety net: yes".

The Government can change the concession status on your record in the SCRS without you being present. (For example, if your circumstances change and you no longer receive a particular welfare or veteran's benefit, the concession status flag would be changed from 'yes' to 'no'.) This change can then be 'uploaded' to the chip on your card, the next time you insert your card into an appropriate reader.

However until the information on the chip in your smartcard is actually checked for currency against the SCRS, it is no better than the current system of paper cards and/or online checking.

Q: Whose readers will be capable of connecting to the SCRS to check the currency of concession status information on the chip, and change that information by way of 'upload' where necessary?

Q: Will third party government agencies and businesses have to also check the backend database (SCRS) in order to be able to determine the current validity of a customer's concession status?

Q: Does that mean that every time I want to claim a concession benefit - from buying PBS safety net medicines at the chemist to buying a bus fare or a move ticket or paying my council rates or water bills – the government agency or business will be connecting to check my record against the SCRS, or a against 'blacklist' of recently-cancelled concessions 'pushed out' to smartcard readers from the SCRS?

Q: Will the Government therefore get a log of every time I have claimed a concession fare or discount, even if the concession doesn't relate to DHS or DVA?

## *Claims about data accuracy (fixing errors)*

Q: What % of the estimated up to $3 billion in financial savings relates to reducing errors made by DHS and DVA agencies?

We don't know. The Government has just claimed that "KPMG has found that the introduction of the access card would lead to substantial cost savings from improved efficiencies, and a reduction in identity fraud, abuse of concession entitlements and errors. KPMG estimate the savings could be as much as $3 billion over ten years" (*Fact Sheet (Financial Case)*, DHS website).

Q: What % of the estimated up to $3 billion in financial savings relates to reducing errors made by Centrelink alone?

The Australian National Audit Office (ANAO) has recently reviewed the integrity of Centrelink's records (Audit Report No. 29, 2005-06), Medicare enrolment data (Audit Report No. 24, 2004-05), and Medicare cards (Audit Report No. 54, 2004-05).

The ANAO found that up to 30% of customers' identity information held by Centrelink is not sufficient to uniquely identify or authenticate customers, which could impact on fraud detection (KPMG Report, p.7).

KPMG has also identified that between $75 million and $150 million annually is being overpaid by Centrelink to people who are recorded in their own records as dead (KPMG Report, p.7).

Q: Was amalgamating 17 cards into one recommended by the Australian National Audit Office as one of its recommendations for improving data accuracy / integrity in Centrelink and/or Medicare?

No.

Q: Have all recommendations by the Australian National Audit Office for improving data accuracy / integrity been implemented by Centrelink and Medicare?

Q: Why shouldn't these other, more targeted recommendations from the Australian National Audit Office be implemented and evaluated prior to introducing a far more intrusive and expensive project with the same objectives?

## *Claims about the system being 'voluntary'*

Q: Is this system voluntary?

It might be in law, but not in practice.

You will need to have the ID Card with you to receive bulk-billing healthcare, to receive Medicare rebates on other health services, to receive PBS-subsidised medicines, to receive any social security benefits, from the baby bonus to Austudy to the aged pension, and to receive concessions or discounts on a range of goods and services, such as public transport, council rates and utility bills.

So to access health or social security or concession benefits, getting the Card, and being registered on the national population database, is compulsory.

Professor Allen Fels, Chair of the Consumer and Privacy Taskforce has already said that the Government's claim about the card being 'voluntary' do not stack up: "the Taskforce recognises that, at some stage, almost every Australian is likely to need an access card" (Taskforce Discussion Paper, p.19; see also "Warning on ID card by stealth", *Herald Sun*, 17 June 2006).

In particular, the Consumer and Privacy Taskforce has already warned the Government that it is "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" (Taskforce Discussion Paper, p.16).

Q: How many people does the Government expect to get a Card?

All 16.5 million adults: "we need to plan on the basis that all those who are eligible for it will seek to take it up" (Budget Estimates, p.54). In effect, the Government is assuming, and budgeting for, every adult to get the ID Card.

The only people who don't need to register for the card are people "who elect to pay full fees for Medicare services and do not wish to claim a concessional benefit, Centrelink entitlement, or PBS safety net access" (KPMG Report, p.29).

So even the Government doesn't really believe this card is 'voluntary' in a true sense – they know everyone, except perhaps the mega-wealthy, will need one. That means only privacy for the rich.

Q: Why isn't the new Card optional for accessing social security or concession benefits?

KPMG found that a "sound value proposition" for the proposal only exists if the Card is made compulsory for access to any DHS or DVA benefit (KPMG Report, p.10).

A clue to why is found on p.15: "any assumptions about fraud savings … would be negated if the system were voluntary" (KPMG Report, p.15).

Q: If the system is voluntary, does that mean people can opt in or out at any time?

It doesn't look like it.

The KPMG report suggests that once a person is registered, their "registration and POI will last them throughout the rest of their life" (KPMG Report, p.15). No mention is made of 'opting out' of the system, for example if you leave Australia, or decide you can afford to never rely on Medicare or social security benefits.

Officials giving evidence before the Senate suggested that while people could 'opt out' of the system, they did not know whether that meant their data would be deleted from the SCRS (Budget Estimates, p.87).

Q: Can your card be cancelled against your will?

The Consumer and Privacy Taskforce has said that "it is possible that confiscation of access cards may be authorised by law in the event of their systematic or criminal misuse" (Taskforce Discussion Paper, p.14).

Q: In what circumstances will the Government confiscate people's access cards?

Q: What measures will be put in place to deal with the problems of "identity denial", which could lead to the denial of health and social service benefits from 2010, for people whose access card has been confiscated by the Government?

## *Claims about biometrics photographs and facial recognition*

Q: What's the difference between a digital photograph and a biometric photograph?

A digital photograph is just a "digitised" photograph, and something many people would be familiar with – a photograph taken with a digital camera, or a 'hard copy' photograph scanned into a computer.

By 'biometric' photograph what is normally meant is that the digitised photograph of a person's face is then used to collect certain features about that face, such as the distances between eyes, nose, cheekbones, etc. Using a mathematical formula (an algorithm, these measurements are then turned into a "template" (a reduced biometric dataset), which can be stored separately to the digital photograph. The template can then be used to compare against other templates produced from measurements taken from other people's faces, either live or from other photographic images.

Q: How does facial recognition work?

Facial recognition technology can enable one or more of the following:

- Live identification: a live person is photographed, and their "template" checked against millions of templates of other people in a database. This is one-to-many matching, which yields a set of possibilities. It requires a scanning machine to scan the live person's face, and the algorithm to turn measurements into a template. This would be used to check whether that live person was already enrolled in the system under that or another name.

- Photo identification: a photo on a document is checked against millions of photos of other people in a database (one-to-many matching). The photograph has to be reduced to a template first.
- Live verification (a): a live person is photographed, and their "template" checked against the template produced from their photo on a document they are holding. This is one-to-one matching, which yields a 'yes' or 'no' answer. This requires a scanning machine to scan the live person's face, and the algorithm to turn measurements into a template.
- Live verification (b): a live person is photographed, and their "template" checked against the template produced from their photo in a database. Again this is one-to-one matching, and requires a scanning machine to scan the live person's face, and the algorithm to turn measurements into a template.
- Photo verification: the template from a photo on a document is matched against the template from a photo listed against the same person in a database.

Q: Can a person's ethnicity be determined from their biometric template?

Q: Is the biometric photograph proposed by the Government intended for facial recognition at the time of registration, or at the time of service delivery?

It is fairly clearly intended to work at the time of registration (see below under 'Facial recognition at registration'); but it is less clear about whether it will be used from that point forward (see below under 'Facial recognition at time of service delivery').

Q: How feasible is one-to-many matching, using facial recognition to match against a database of millions of photos?

The Australian Customs Service originally tried one-to-many matching at airports, in their SmartGate 1 trial. This tested matching a live person against all the images of passport-holders in their database. Even with the small number of images held in their database (testing was only being done on airline crew), this system was not found to be feasible, and therefore is not being adopted on a large scale.

Therefore SmartGate 2 now only does one-to-one matching, in which a live person is checked against the photograph in their e-Passport – a process which takes about 6 seconds.

However the Department of Foreign Affairs and Trade, which issues the e-Passports, is conducting one-to-many matching at the time a person first applies for a new passport. That is, they check a person's photo (from their passport application form) as against all the photos of passport holders they already have in their database, to see if that person already has a passport issued in another name.

Therefore, facial recognition is now being used:

- by DFAT for once-off *photo identification* (checking: "who is this person?") by conducting a one-to-many check, at the time of applying for an e-Passport), and
- by Customs for transaction-based *live verification* (checking: "is this person who they say they are?") by conducting a one-to-one check, at the time of walking through an airport or seaport.

Q: What is the algorithm, or method, to be used to create the biometric template from a photograph?

## *Scope of costs*

Q: What is the proposal likely to cost?

> The Government has claimed that "The cost of establishing the access card is $1.09 billion over four years" (*Fact Sheet (Financial Case)*, DHS website).

Q: What is the 'best case scenario' figure on estimated costs by KPMG?

Q: What is the 'worst case scenario' figure on estimated costs by KPMG?

Q: What is the 'most likely scenario' figure on estimated costs by KPMG?

Q: What has the Government budgeted for the proposal?

> The 2006-07 budget, announced 9 May 2006, allows $1.09 billion over four years, from 2006 to 2010. Divided by the 16.5 million adults estimated to receive the card, that's about $66 per person.

Q: How much of the budget is for the actual card?

> KPMG have said a smartcard is estimated to cost $7.50 per card (KPMG Report, p.24).
>
> That suggests $123,750,000, or more than 10% of the project's costs, is required to issue 16.5 million cards to start with, and the same again every seven years as the cards expire and need replacing.

Q: How much of the budget is for establishing a national smartcard infrastructure?

> The Minister, Joe Hockey, has said that his project will "roll out new infrastructure (which will) provide a platform others can build on" ("Minister flags e-purse on ID smartcard", *The Australian*, 4 July 2006).
>
> Slated users of a national smartcard infrastructure include banks, driver licensing authorities, public transport ticketing authorities, convenience stores, toll-road operators, libraries and event/venue ticket vendors ("States' move boosts smartcard", Australian Financial Review, 5 July 2006).

Q: Will banks and other corporate users benefit from the establishment of a national smartcard infrastructure?

Q: If banks and other corporate users will benefit from the establishment of a national smartcard infrastructure, why haven't they invested in developing the infrastructure themselves?

Q: If the banks and other corporate users aren't willing to invest in a national smartcard infrastructure themselves, but will benefit from it, does this mean that taxpayers will be subsidising banks and other corporates?

Q: Will the costs of establishing a national smartcard infrastructure come out of the DHS health and welfare benefits budget, or will banks be asked to contribute?

Q: How much of the budget is for card readers?

> The business case prepared by KPMG suggests that not all health service providers will have readers capable of displaying a photograph, and that the "cost of providing readers capable of displaying photographic images for all providers in the DHS service system would be high" (KPMG Report, pp.17, 19).
>
> However Government officials have claimed that the Government is planning to supply uniform readers to "doctors and others", and that this is part of the budget (Budget Estimates, p.78).

Q: How much of the budget is for the registration process?

> "a very significant proportion of the costs of the project is to do with registration, including the staff based effort to meet with all those people" (Budget Estimates, p.88).

Q: How much of the budget is for capital?

> The budget has allocated $80 million in capital over the four years, across Medicare Australia, Centrelink, the CSA, Veterans Affairs, the Department of Family, Community Services and Indigenous Affairs, and the Department of Human Services, "for internally developed software, hardware and some property costs" (Budget Estimates, p.51).

Q: How much of the budget will be spent on 'communications strategy'?

> The 2006-07 budget includes $47.3m for a communications strategy, comprising $6.5 million in 2006-07, $20.6 million in 2007-08, $8.5 million in 2008-09, $4.9 million in 2009-10; and $7 million split across the DHS and DVA agencies for 'internal communications' (Budget Estimates, p.53).

Q: Given registration will not commence until *at least* 2008, why is $6.5 million needed in 2006-07, and $20.6 million in 2007-08?

Q: What will the content of the advertising be?

Q: What will the timing of the advertising be, in relation to the next federal election?

Q: How much of the budget is for the consumer and privacy taskforce?

Q: Is the budget of the consumer and privacy taskforce part of the $47.3 million 'communications strategy' component?

Q: Are there any other costs associated with the proposal that have not been counted in the $1.09 billion costings?

> Yes. A total of $3.6 million was spent by DHS to June 2006 on the work of the smart technologies task force (Budget Estimates, p.86). About $2.1 million has already been spent on external advisers including KPMG ($1.944 million) and Clayton Utz

($127,000). This was before the $1.09 billion budget was approved, and came out of different funds.

Q: How much of the $3.6 million already spent was on overseas trips for DHS staff and/or external advisers engaged in preparing the business case for the so-called access card?

## *Scope of financial savings for the Government*

Q: What are the estimated financial savings from the proposal?

The Government has claimed that "KPMG estimate the savings could be as much as $3 billion over ten years" (*Fact Sheet (Financial Case)*, DHS website).

Q: What is the 'worst case scenario' figure on estimated financial savings given by KPMG?

We don't know; the Government won't tell us.

Q: What is the 'most likely scenario' figure on estimated financial savings given by KPMG?

We don't know; the Government won't tell us. The business case states: "Detailed costings have been removed for commercial reasons" (KPMG Report, p.12).

However we do know that KPMG has warned the Government both of the risk of "overstating the benefits", and the risks facing this proposal based on the "history of unrealised returns and benefits in many large scale projects of this kind" (KPMG Report, p.13).

Q: Where will the financial savings come from?

Departmental officials have said "the savings in outlays would arise … principally around fraud reduction, proof of identity and photographic proof of who you are", with only "some minor departmental savings in some of the agencies" (Budget Estimates, p.60).

## *The likelihood of 'function creep'*

Q: What additional features have been mooted?

The Minister has noted that while some have called for the card to double as a repository of electronic health records, he has rejected this request. He has however suggested that electronic prescription / pharmacy applications would be contemplated: "there may be room for a later debate about electronic scripts being stored on the card" (Joe Hockey speech to the AMA National Conference, 27 May 2006).

The KPMG Report suggests the card could work as an electronic wallet, not only for one-off payments such as disaster relief, but also "to enable consumers to access specific funds" (KPMG Report, p.10).

The so-called access card has also been mooted as the key to parents' daily access to child-care centres? (According to a media report, the Government has approved a $50 million software system, to be run by the Department of Family and Community Services, to track use of child-care down to the individual child ("Child ID cards in swipe

at fraud", *Sydney Morning Herald*, 2 June 2006). The report says parents will be issued with swipe cards or PINs, needed to clock their children in and our of child-care centres.) Government officials have said "that is not decided yet" (Budget Estimates, p.94).

Q: What has the Government proposed to prevent 'function creep'?

Absolutely nothing.

The consumer and privacy taskforce has already said that legislation would be needed, along with other safeguards, to prevent the so-called access card from becoming a national ID card ("Warning on ID card by stealth", *Herald Sun*, 17 June 2006). And even KPMG warned of the risk of function creep (KPMG Report, pp.13, 32).

Yet government officials have noted the absence of any limits, stating that any change in function would merely have to be "either requested by consumers or a decision of government" (Budget Estimates, p.73).

Furthermore, no limitations are proposed on who may ask to see your ID card, or copy your card's ID number.

# The Card

## *Card registration*

Q: Who will need to be registered?

Both adults and children/dependents will be registered (KPMG Report, p.14). However, while details of "dependents will be stored on, or linked to, the smart chip of the parent or guardian's card", there will not be a photograph taken of dependents, unless they request their own card (KPMG Report, pp.14, 16).

Q: Who will need to get a card?

All adults, plus any children who request their own card. Children who request their own card will presumably be required to have their photograph taken also.

Q: What is the definition of an 'adult' for this proposal?

In discussions the Department has said 18, but the KPMG Report suggests it examined the proposal based on calculations for those "over the age of 15" (KPMG Report, p.11).

Q: Will people be required to pay a fee to get the card?

The Government has said "it is unlikely that there will be a cost" (Budget Estimates, p.95).

Q: Will people be required to pay a fee to replace their card if it is lost or stolen?

It's not clear: "unlikely … But those decisions are not made (yet)" (Budget Estimates, p.95).

Q: What is the basic registration requirement?

"There will be a range of documents that (people) will need to present and … you will also be required to have a photograph taken under controlled conditions" (Budget Estimates, p.95).

However there will not be a photograph taken of dependents (KPMG Report, p.16).

Q: Where will people go to register?

The KPMG costings are based on the assumption that 9.5 million people would attend a Medicare office, and 6.5 million would attend a Centrelink office, "with other outlets providing additional services where required" (KPMG Report, p.30).

2.3% of Australians live more than 50km from a Medicare or Centrelink office (Budget Estimates, p.86). Other possibilities being examined include Australia Post outlets ("Cast of thousands the tip of Access iceberg", Computerworld, 21 June 2006, p.30).

The Consumer and Privacy Taskforce has also raised the issue of how registration might work for Australians resident overseas.

Q: What documentation will be required for registration?

The Government states that details about the documentation required to register for the so-called access card "will be made available closer to the registration period" (*Access card at a glance*, "How do you obtain an access card?", DHS website).

The Government claims the documentation required to complete the card registration process will "take into account the needs of … rural and remote communities, the elderly and the mentally ill" (*Access card at a glance*, "How do you obtain an access card?", DHS website). No mention is made in the DHS literature of indigenous communities or homeless people, who often have few, if any, existing identification documents.

Q: How will registration work for indigenous communities or homeless people, who often have few, if any, documents that can add up to establish their identity?

The KPMG Report mentions mobile registration teams to assist people who are homeless, house-bound, or who have difficulty establishing their identity through existing documentation.

However they also note that people who cannot meet the minimum standards of registration information should have a "low POI confidence flag" attached to the chip in their card (KPMG Report, p.52).

Q: What measures will be put in place to deal with the problems of "identity denial", which could lead to the denial of health and social service benefits from 2010, for the likely indigenous and homeless people to receive a "low POI confidence flag"?

None as yet that we can see.

However the Consumer and Privacy Taskforce has also noted that "care must be taken to balance the need for identity verification at the highest level with the possibility that this could exclude access by those most in need" (Taskforce Discussion Paper, p.24).

Q: If the customer registration requirements are relaxed for indigenous and homeless people, how will this meet the project's objective of producing a high-integrity, government-issued identification document?

KPMG has warned the Government that it can't do both: "Any inadequacies in (the) registration process and the initial POI requirements will be entrenched in the system. This has the potential to undermine the capacity to address fraud if not handled properly" (KPMG Report, p.48).

This is why they recommended that people who cannot meet the minimum standards of registration information should have a "low POI confidence flag" attached to the chip in their card (KPMG Report, p.52).

This sounds like second-class citizenship to us.

Q: What is the estimated rate or risk of entrenching current false identities?

Q: What is the estimated dollar value of identity fraud and identity theft likely to be generated by this project, as a result of entrenching current false identities?

Q: What measures will be put in place to deal with the problem of "identity theft", arising when a legitimate person arrives to register for their so-called access card, only to find that there has already been a fraudulent registration by a different person using their name and/or documentation?

Q: On what basis can a card be cancelled or withdrawn against the card-holder's will?

Q: How many minutes has been estimated for registration?

> The Department of Human Services has been quoted as saying it estimates that "it will take at least 15 minutes an application for each smartcard" (James Riley, "ID card to boost IT funds", *The Australian*, 9 May 2006).

Q: If it is not yet known or determined what documentation will be required for registration, how can time (and therefore cost) estimates have been conducted on how long registration will take?

Q: Will copies of registration documents be kept by DHS?

> It would appear so. Officials giving evidence before the Senate said: "There will be a range of documents that (people) will need to present and which we will scan, store and verify" (Budget Estimates, p.95).

Q: Will I ever need to go through this process again?

> Every seven years you will need to turn up to get a new photo taken and be issued with a new card.

## *Facial recognition at registration*

Q: Will facial recognition technology be used to identify people at the time of *registration* for the card?

> It would appear so. KPMG recommended: "It is proposed that the photo be capable of digital matching to prevent duplicate issuance of cards" (KPMG Report, p.16).
>
> One government official giving evidence to the Senate stated: "The thinking is we would take the photograph under controlled conditions at the registration process. That photograph would be on the card, in the chip, and on the database" (Budget Estimates, p.75).
>
> A second official then stated: "in the event that someone sought to achieve two such cards from the same physical appearance that ought to be detected. … The whole intention is that at the point of capture when people register for the card that image will be able to be checked against the database of images and I will not be able to get two cards with my one face" (Budget Estimates, p.76).

Q: What is the estimated error rate (both false positives/matches and false negatives/rejects) from the automatic facial recognition technology to be adopted in DHS / DVA offices?

> The KPMG Report notes that biometrics "generate some level of false rejection and false acceptance", but does not quantify the error rate for the facial recognition technology it recommends (KPMG Report, p.22).

Large scale test results from the UK Passport Service in 2005 found that facial recognition was the least successful identification technology, with an overall success rate of only 69% accuracy in verifications. This success rate dropped for people aged over 60, as well as for people whose appearance had changed in the period between enrolment and subsequent verification. For people who had been registered at mobile centres, the success rate dropped to 48% (UK Passport Service, Biometrics Enrolment Trial, Management Summary, May 2005, p.8).

Q: Will the Government specify a minimum performance requirement with respect to false *rejections* during registration?

A false rejection in this context means the SCRS not matching two images that should have been matched, because they were from the same person. A false rejection would allow a person to be registered twice, under different names.

A false rejection rate of 1% means that in 1% of cases where a person is attempting to fraudulently register on the SCRS a second or subsequent time, the system fails to detect their fraud by realising that the biometric templates match.

A false rejection rate of 1% would be exceptionally low by industry standards. However this would still mean thousands of people could commit identity fraud or identity theft, without being detected by the system.

There is a practical difficulty in monitoring the false rejection rate, because it is impossible to tell how many times the system lets a person through who should have been spotted.

Q: Will the Government specify a minimum performance requirement with respect to false *matches* during registration?

A false match in this context means the SCRS wrongly matched two images that should not have been matched, because they were from two different people.

A false match rate of 1% would be exceptionally low by industry standards. However this would still mean 165,000 people being accused, falsely, of being an imposter.

Q: How will the Government deal with matches during registration, to determine whether or not the match is accurate or false?

The Government has yet to detail the exact registration process. In particular, the Government should explain whether it will require people to undergo longer interviews, succumb to inspections or questioning of family members or associates, or return with further evidence of identity.

KPMG has recommended that people who cannot meet the minimum standards of registration information should have a “low POI confidence flag” (KPMG Report, p.52).

Q: Will people who have the required documentation for registration, but whose face throws up a ’match’ against another face on the database, be instead issued with a card showing a “low POI confidence flag”?

Q: Will people already registered be recalled for questioning if a subsequent person’s registration throws up a ‘match’ against their photograph?

Q: How will this system deal with people of similar physical appearance, including identical twins?

Q: How will this system impact on people being registered at mobile locations?

> Trials of facial recognition technology by the UK Passport Office found that "(m)aintaining the correct position for facial biometric enrolment was a problem for some Disabled participants with a physical impairment or with learning disabilities" (UK Passport Service, Biometrics Enrolment Trial, Management Summary, May 2005, p.7).
>
> Furthermore when it came time to utilise the biometric template produced at mobile enrolment centres, for the purposes of verifying identity against a database of photographs, the success rate dropped to 48%. The report of the trial suggested this could have been due to poor lighting in mobile enrolment centres (UK Passport Service, Biometrics Enrolment Trial, Management Summary, May 2005, p.8).
>
> This suggests that people registered at mobile sites will be more likely than the general population to be the subject of a false match, and thus be falsely accused of being an imposter. This will likely impact disproportionately on people with disabilities, the frail aged, indigenous and homeless people – the very people who will have great difficulty producing further evidence of their identity to demonstrate that the match was false.

Q: What is the estimated shelf-life of the so-called access card, given the changes in facial features that can occur over a 7-10 year period?

> We don't know – the technology hasn't been around long enough to be sure.
>
> Biometric photographs, suitable for a person-to-document match, have only just been introduced into Australian e-Passports, issued from October 2005. The likelihood of these photographs progressively failing over the life of each 10-year passport (as people's facial features change with age, and/or as the chip ages or is damaged through wear and tear) is therefore not yet quantified.
>
> Trials of facial recognition technology by the UK Passport Office found that the overall success rate of 69% verifications dropped for people aged over 60, as well as for people whose appearance had changed in the period between enrolment and subsequent verification – a period of only some months in their trial (UK Passport Service, Biometrics Enrolment Trial, Management Summary, May 2005, p.8).

Q: What measures will be put in place to deal with cases of "identity denial" (registration denial), based on false negative readings from the facial recognition technology?

> While acknowledging this very real possibility, KPMG fudged a non-answer by leaving this one to the Government: "business rules would need to be established within the SCRS to determine how to manage cases where a unique high-probability match could not be achieved"; options could include asking for another form of "proof of identity", taking another photograph, or accepting the risk of a lower level of certainty about the uniqueness of that person's identity (KPMG Report, p.22).

## *The information on the card*

### The face (and back) of the card

Q: What information will be visible on the face (or back) of the card?

The face of the card will show your name and photograph, and the back of the card will have your signature and card number (DHS website, http://www.humanservices.gov.au/access/index.htm ).

Q: If there is going to be a photograph on the chip (see below), why is it necessary to have the photo displaying on the card too?

If the only people who needed to use the card to verify your identity were DHS and DVA customer service staff, the photograph wouldn't be necessary at all – the DHS and DVA staff could simply use their reader to look at your photo.

But unfortunately the Government has designed this proposal with not only the core DHS and DVA customer service transactions in mind. The photo is promoted by KPMG as necessary, not because DHS or DVA need it for customer service, but because of the *optional* extra features being promoted for the card – its use to display health information to emergency workers, and its use as an all-purpose proof-of-identity card (KPMG Report, p.17).

Q: How will a photo on the face of the card assist a pharmacist dispensing medicine, or an emergency worker such as a paramedic, if they need a card reader to see my health information anyway – can't they read the photograph from the chip as well?

The business case prepared by KPMG suggests that not all health service providers will have readers capable of displaying a photograph, and that the "cost of providing readers capable of displaying photographic images for all providers in the DHS service system would be high" (KPMG Report, pp.17, 19).

However Government officials have claimed that the Government is planning to supply uniform readers to "doctors and others", and that this is part of the budget (Budget Estimates, p.78).

Q: If the Government is going to supply uniform readers to health service providers who might need to access the volunteered emergency and health information, and those readers will be capable of displaying a photograph from the card's chip, why is a photograph needed on the face of the card at all?

Q: If the photograph on the face of the card is intended as a 'backup' for blackouts or other situations with no electricity to run a reader, how can the other necessary details (such as PSB safety net status) be validated from the card's chip for information to be processed anyway?

Q: If the Government is *not* going to supply uniform readers to health service providers who might need to access the volunteered emergency and health information, does this mean key privacy protections have been dumped in favour of cost savings?

Q: If a photo on the face of the card is still intended for third party applications outside the health and social security sectors, such as a general proof-of-identity for banks, video rental stores, etc, why not make this an optional feature for people who don't have driver's licences as a ready alternative?

Q: Has the Government recognised that having a photo displayed on the card increases the likelihood the card will become a defacto national ID card?

The Government seems to want to have it cake and eat it too – on the one hand, claiming this is not a national ID card, but on the other, designing and promoting it as an

all-purpose proof-of-identity card, suitable for a range of purposes entirely unrelated to accessing health or welfare benefits.

However in developing the 'business case' for the Government, KPMG dismissed concerns raised by privacy advocates about the impact of introducing a new photograph-based identity document, on the basis that drivers' licences and passports already have photographs (KPMG Report, p.18).

It would appear that KPMG did not grasp the implications of introducing a new, *universal* photo ID card, which also incorporates a unique and universal number. This will significantly increase the likelihood of photo ID being routinely demanded by a variety of government agencies and businesses, and will in turn lead to the national ID number being recorded and used in a variety of ways, entirely unrelated to accessing health or welfare benefits.

Perhaps this is because KPMG did not actually meet with privacy advocates in its alleged "extensive stakeholder consultations", but instead relied on second-hand comments from DHS staff, based on previous consultations held to discuss a different model altogether.

## Chip contents

Q: What information will be stored on the chip?

The card's computer chip will contain address, date of birth, concession status, a signature, a photograph and the names of children and other dependents, and optional information, "such as emergency contact details, allergies or things like that" (Budget Estimates, p.73).

KPMG recommended that "Details of dependents will be stored on, or linked to, the smart chip of their parent or guardian's card" (KPMG Report, p.14).

Q: Why would the photograph be needed on the chip as well as the face of the card?

KPMG recommended this, "to enable validation of the image where the face on the card might have become worn/damaged or where there might be suspicion that the card has been tampered with in some way" (KPMG Report, p.17).

Q: If a card had become worn or damaged, shouldn't it just be replaced?

Q: If a DHS officer suspected a card's photo had been tampered with, couldn't they check it against the SCRS database?

Q: Why would the signature be needed on the chip as well as the face of the card?

Q: What information will be stored on 'my' card's chip for each of my children or listed dependents: e.g. will it include their card number (whether for issued or unissued cards), SCRS ID number, name/s, date of birth, gender, birth parents, relationship to me, whether a current/active relationship, and relationship start/expiry dates?

## Accessing the chip contents

Q: Who will be able to 'read' the contents of the chip?

This hasn't yet been defined, and the Government has been vague about the issue of encrypted readers for authorised parties.

KPMG has said that "agencies or service providers that have readers with a suitable display device (integrated or connected) can display the photo to confirm the cardholder identity" (KPMG Report, p.17).

However when asked by Senators whether commercially available smartcard readers bought off-the-shelf from Dick Smith would be able to read the contents of the card's chip, Government officials said "We do not know yet. It is not decided. We do not know the exact nature of the card and whether those sorts of readers will be able to be used" (Budget Estimates, p.94).

Q: How will information on the chip be protected?

KPMG has proposed the chip contents be divided into a 'public zone' and a 'closed zone', with information in the closed zone PIN-protected. However it would appear that there is in fact a third point of access, allowing authorised people to read information in the 'closed zone', even without a PIN.

It is not clear which bits of information will be 'public', and which will be PIN-protected. KPMG has noted that "anything stored in the 'public zone' is potentially vulnerable to being captured electronically without the permission of cardholders" (KPMG Report, p.19).

Q: Who will be able to access the 'emergency' information, and in what circumstances?

One Government official has claimed that the optional information, "such as emergency contact details, allergies or things like that", will be "protected by a PIN" (Budget Estimates, p.73).

We think that is most likely incorrect. PIN protection is of course counter-productive in the very type of emergency this would be designed for – you are unconscious after a car accident, and a paramedic needs to know if you are allergic to pethidine. If you're physically unable to tell someone about your allergies, you are even less able to remember and input a PIN.

Yet if emergency health and contact details are placed in the 'public zone' of the chip, not only will ambulance officers be able to read it, but so will Centrelink staff, bus ticket sellers, and anyone else who inserts your card into their reader.

Q: Will people be able to suppress their home address so it is blocked from view of most or all readers of the card?

Q: Will people be able to suppress their health and emergency contact information so it is blocked from view of all readers of the card except emergency medical personnel?

## Chip specifications

Q: What standards will be used to determine the chip's appropriateness, utility, security, etc?

> The Government has stated that the chip will confirm to "international standards" (*Fact Sheet (Technology)*, DHS website). It hasn't specific what standards it is referring to.
>
> However KPMG has noted that "anything stored in the 'public zone' is potentially vulnerable to being captured electronically without the permission of cardholders" (KPMG Report, p.19).

Q: Will the chip's design be subject to an independent assessment and certification process, such as the CCEVS (Common Criteria Evaluation and Validation Scheme for IT Security) process offered by the National Institute of Standards and Technology and the National Security Agency in the US, to ensure it conforms to international standards?

Q: What size chip will be used?

> It's not clear. The Minister has on various occasions referred to the chip being 64 kilobytes, or KB (Joe Hockey speech to the AMA National Conference, 27 May 2006). However he's also mentioned smaller sizes such as 32KB, or much bigger sizes (e.g. 64MB – a megabyte is roughly 1,000 times bigger than a kilobyte). The reference to 64MB appears to have been an error.
>
> However it is worth questioning whether some of the proposed features (such as a biometric photo of the sufficient resolution required for one-to-many facial recognition technology) will actually fit on a 64KB chip. If bigger chip sizes are needed, then the cost estimates for the project will presumably be affected.
>
> For example, Australia's new "e-Passports", which store a biometric photograph of the sufficient resolution required for facial recognition technology, as well as some limited identity information, are now operating on a chip of 512KB.

Q: Is it proposed to be a contact, contactless or combined contact / contactless smart card?

Q: How much chip size will be for dynamic memory (erasable non-volatile memory, used for storing erasable data, and can retain data when no power is available)?

Q: How much chip size will be for static memory (non-erasable non-volatile memory, used for storing applications)?

Q: How much chip size will be for volatile memory?

Q: What applications will be built into the chip?

Q: Can/will applications on the card be changed dynamically, i.e. after the card is issued?

Q: What encryption type and level will be used on the chip?

Q: What encryption type and level will be used for transmissions to and from the card's chip?

Q: How many discrete applications will be supported on the card's chip, and what are they?

> The Government's proposal is not for simply a data storage card – the proposal includes payment, access and potentially other applications involved.

Q: Will the source code for the chip's applications be made available for independent inspection and review, to reveal any surreptitious applications or covert data retention?

Q: With respect to payment applications using the card, will they use a standard financial institution payment application like EMV, or something proprietary to this particular card?

Q: Why is the Government not waiting for AGIMO's smartcard framework to be rolled out before designing this system?

## Biometric photograph on the chip in the card

Q: Will the card's chip contain a photograph?

> Yes. The card's computer chip will contain address, date of birth, concession status, a signature, a photograph and the names of children and other dependents, and optional information, "such as emergency contact details, allergies or things like that" (Budget Estimates, p.73).

Q: Will the photograph be a digital photograph or a biometric photograph?

> It would appear both.
>
> The Government has stated that "The access card will contain … a biometric photograph. … A biometric photograph can be translated into a mathematical algorithm and used to test for similarity of appearance against the biometric photographs of other people…." (*Fact Sheet (Technology)*, DHS website)
>
> (Note however that the algorithm is not the set of numbers derived from a photograph, it is the method for doing the reduction. The proper term for the reduced biometric dataset is a "template".)

Q: What resolution will the photograph be?

Q: Will the photograph be of a sufficient resolution to enable automatic one-to-many matching (i.e. automatic matching against a database of photographs), as opposed to one-to-one matching (i.e. humans to verify by sight that the person presenting matches the photograph on the card)?

Q: How much memory on the chip is required to store a biometric template, compared to just a digital photograph?

Q: Were the KPMG costings based on a chip size sufficient to store this volume of data?

Q: Will there be any identifiers stored inside the card's chip, beside the card number (found on the face – or back – of the card)?

Q: If so, what existing identifiers will be held (e.g. existing client numbers for DHS agencies, and/or any new identifiers)?

Q: If so, how will those identifiers in the chip going to be encrypted?

## *Using the card at DHS and DVA*

Q: The card will be compulsory to receive health and social services benefits. What is the full scope of what is meant by "health and social services benefits"?

> The Government has stated that the card "can be used to access benefits at Medicare, Centrelink and the Department of Veterans' Affairs" (*Access card at a glance*, "Where can the card be used?", DHS website).
>
> The Government has also stated that, from 2010, "you will need an access card to continue to access health and social services benefits" (*Access card at a glance*, "Who needs an access card?", DHS website).
>
> However the Department of Human Services actually comprises six agencies: Medicare and Centrelink, plus the Child Support Agency, CRS Australia (rehabilitation services), Health Services Australia, and Australian Hearing.

### Customer identification

Q: Will the so-called access card also be used as the key customer identification tool for the other four DHS agencies (i.e. Child Support Agency, CRS Australia, Health Services Australia, and Australian Hearing)?

> Yes. Evidence before the Senate confirmed that the CSA is a major player, so "if you are going to be involved in the child support system, you will need to have one of these cards by 2010"; and the card will be needed for "all DHS agencies and the Department of Veterans' Affairs" (Budget Estimates, p.87).

Q: Will the so-called access card be used as the *only* customer identification tool for all six DHS agencies, from 2010?

Q: What will prevent cases of service denial – i.e. DHS and DVA officials who deny services to ill or destitute people who have lost or forgotten their card?

> It would seem the Government doesn't know: "We have not worked out all those details yet" (Budget Estimates, p.79).

### Facial recognition at time of service delivery

Q: Will facial recognition technology be used to identify or verify people at the time of accessing services (as opposed to at the time of registering for their card)?

To date the Government appears a little confused about what "facial recognition" and "biometric photo" really means in the context of service delivery, and is covering its bases by saying your photo will be on the face of the card, on the chip in the card, *and* on the centralised SCRS database.

For example Government officials giving evidence to the Senate stated: "When the customer presented that card into a reader at the desk that photograph would be checked against the database. If there were a mismatch then that would raise an alarm" (Budget Estimates, p.75).

This suggests that at the time of service delivery (e.g. while visiting a Centrelink office), the photograph on the card will be checked to see if it matches the photograph for the same person, as held on the SCRS. This one-to-one matching only tests for whether or not the card is a forgery, not whether or not the person holding the card is the right person.

However KPMG warned that "use of biometric identification at the point of service provision is not regarded as necessary … (because) it will add to the cost… it will inconvenience customers and service providers and it will be highly contentious from a privacy perspective" (KPMG Report, p.21).

Q: Will DHS / DVA use 'automatic' facial recognition (i.e. a machine does the check) to check that the person presenting before them matches the photograph of the person listed against that name or DHS ID number on the SCRS?

Q: Will DHS / DVA use 'manual' facial recognition (i.e. the officer does a visual check) to check that the person presenting before them matches the photograph of the person listed against that name or DHS ID number on the SCRS?

Q: If officers are going to check the person as against their photograph in the database, why does the card also need a photograph?

Q: What account has been taken of the theory that photographs add little security benefit to cards, as they are not scrutinised routinely?

Q: How will a photograph be of any assistance if the customer is conducting a transaction online or over the telephone?

## *Using the card in health-care settings*

Q: Currently my GP records my Medicare number on my first visit, then just keeps it on file. Will this change – will I have to bring my card with me every time?

Q: Will medical services be available if I lose my card?

Q: How can I get anonymous medical treatment while using the card?

Both specific health privacy laws and the Australian Standard for patient identification (AS 5017-2002) require that where lawful and practicable, patients should be able to remain anonymous.

Q: What will prevent service denial in the health sector – i.e. health service providers who deny services to ill or destitute people who have lost or forgotten their card?

> It would seem the Government doesn't know: "We have not worked out all those details yet" (Budget Estimates, p.79).

Q: What information will my health service provider be able to 'read' from the chip in my card?

Q: Will health service providers need me to enter my PIN before they can read any information from the card?

Q: Will health service providers be able to read *only* my emergency contacts and emergency health information, or some or all of the other information stored on the chip (such as home address, details of dependents, and whether or not I am a customer of Centrelink or the CSA)?

## *Using the card elsewhere as "proof of concession entitlement"*

Q: How are concession cards used now?

> Holders of some of the current cards that are to be replaced – such as the Centrelink seniors card and the pensioners' concession card – use their cards to demonstrate their concession status to government agencies or private businesses, outside the DHS and DVA group of agencies. These could include public transport ticket sellers and ticket inspectors, movie ticket sellers, local councils (pension rate rebates), utilities (pensioner rebates or discounts), and a range of private businesses which offer seniors and/or concession discounts.

Q: Will concession status appear on the face of the card, or in the chip?

> Concession status information will not appear on the face of the card, but instead will be stored on the card's chip (*Access card at a glance*, "What information will the access card hold?", DHS website).
>
> This suggests that in order to claim any concession benefits from third party governments and businesses, the customer will need to provide their card, and the third party will need a card reader and authorisation to read the concession status information from the card's chip.

Q: How many different organisations across Australia, whether government or business, have been identified as currently offering discounts or rebates to concession-card holders?

Q: Is it intended that these third party government agencies and businesses will use the so-called access card to verify the validity of a person's concession status?

Q: If not, how is it intended that people will demonstrate their concession status, once their cards are taken away in 2010?

Q: Is it intended that these third party government agencies and businesses will be able to determine a customer's concession status by reading it from the card's chip?

Q: If yes, does the $1.09 billion budget allocation include money for these government agencies and businesses to install or retrofit smartcard readers, so that they can verify the validity of the concession status when a so-called access card is presented to them as evidence of that concession status?

Q: Will these third party government agencies and businesses be able to read *only* the concession status information, or some or all of the other information stored on the chip (such as home address and details of dependents, and health information)?

Q: If a concession has been newly granted (or cancelled) by Centrelink due to entitlement changes, how will that information be 'uploaded' onto the chip so the chip only has current information about concession status?

Q: Will third party government agencies and businesses have to also check the backend database (SCRS) in order to be able to determine the current validity of a customer's concession status?

Q: Will a 'blacklist' of recently-cancelled concessions be 'pushed out' to smartcard readers from the SCRS?

Q: Has the Privacy Impact Assessment specifically examined the likely increased incidence of data-matching and data-mining on customers, across the public and private sectors, that will arise from this so-called access card, given the need for concession-holders to present their card in order to claim any concession-based discounts or rebates?

Q: Has the Privacy Impact Assessment specifically examined the lack of privacy protection afforded customer data once it reaches third party government agencies and businesses?

## *Using the card elsewhere as "proof of identity"*

Q: In terms of third parties using the card as 'proof of identity', will the card be expressly required, expressly prohibited, or something in between?

> Express usage – meaning some organisations outside the health/welfare sectors would be required by law to ask for your card before they provide goods or services – would require a new law.
>
> Express prohibition – meaning organisations outside the health/welfare sectors would be banned from asking to see your card at all – would also require a new law.
>
> At the moment the Government has not proposed any new law. As the Consumer and Privacy Taskforce has noted, "between the poles of express usage and express prohibition lies a grey zone" (Taskforce Discussion Paper, p.22). The 'grey zone' created by the absence of a clear law would still *allow* third parties, outside the health/welfare sectors, to ask for your card before they provide goods or services.
>
> Given concurrent moves by the Government to require a range of businesses to require photo ID be produced before particular goods or services (such as jewellery, real estate, financial services or advice or legal services or advice) are provided, there is a clear 'market' being created for the so-called access card to become the standard means by which 'proof of identity' is established.

Q: Will pharmacists be allowed to request, or require, this card as ID before selling even non-prescription items?

> The Pharmacists' Guild has reportedly already taken it upon itself to demand photo ID of patients purchasing "suspect" items such as cold and flu medicine, and then passing on details to police.
>
> The Sydney Morning Herald reported in April that under 'Project STOP', pharmacists will require buyers of "suspicious" items to produce photo ID, "details of which the chemist then keys into a computer linked to the network. The identification number instantly triggers the display of all recent purchases by the ID holder of suspect products … The system also sends a mobile phone message to law enforcement agencies giving details of a suspect buyer and the time and place of the attempted purchase" ("ID needed for cough drugs as ice targeted", *Sydney Morning Herald*, 7 April 2006).

Q: Will there be a legal prohibition on the card being used by organisations outside the health sector?

> The taskforce has noted that the Government has "*the option* of providing sanctions against any unauthorised organisation or person attempting to demand production of the access card" – in much the same way as there are laws prohibiting people other than employers, financial institutions and the Tax Office from asking for a person's Tax File Number (Taskforce Discussion Paper, p.13; emphasis added).
>
> However the Government is actually promoting the card as an all-purpose "proof of identity" card, with no limitations on who can ask to see it.
>
> The KPMG Report noted that the card would likely be used for work places, clubs and associations (p.16), as well as joining a registered club, applying for a passport, obtaining airline tickets, or purchasing a concession fare on public transport (p.17).
>
> However the Australian Privacy Commissioner Karen Curtis, and Professor Allen Fels, Chair of the Consumer and Privacy Taskforce, have already said that this poses risks, and that legislation would be needed, along with other safeguards, to prevent the so-called access card from becoming a national ID card ("Warning on ID card by stealth", *Herald Sun*, 17 June 2006).

Q: What practical features can be part of a card or number's design, to avoid it becoming an all-purpose "proof of identity" or national ID card?

> When the Tax File Number (TFN) was introduced, it was recognised that as a unique and near-universal identification number for adult Australians, it posed the risk that it could become a defacto national ID number, used by all and sundry as the key through which to track, link and profile so many aspects of people's daily lives.
>
> For this reason significant practical steps were taken to minimise this risk: the TFN was never printed on a card suitable for your wallet; and legislation was passed to prohibit pretty much anyone except the Tax Office, banks and employers from asking you for it.
>
> Likewise when the current Medicare Card was introduced, the cards were allowed to hold the names of multiple family members. Thus the current Medicare card number is not a unique ID number, and so is of minimal value for tracking people's transactions and movements outside the health sector.
>
> These practical protections are not planned for the development of this so-called access card.
>
> Indeed the Government has stated that "cardholders can choose to use the access card as a high quality proof of identity document outside of their interactions with the (DVA

and DHS) agencies, if they so wish" (*Access card at a glance*, "Can I use my access card for anything else?", DHS website).

Meanwhile the Australian Attorney General's Department is overseeing a project to establish common proof-of-identity (POI) documents, to be required by all government agencies when identifying and registering their clients.

Q: Will the so-called access card be *accepted* and/or *required* as one of the common POI documents needed to access services from any Australian government department?

Q: Will the so-called access card be *accepted* and/or *required* as evidence of identity for electoral enrolment, and/or for voting, under the new voting requirements being introduced?

Q: Will the so-called access card be *accepted* and/or *required* in order to obtain a driver's licence and/or buy a vehicle?

Q: Will the so-called access card be used as the key to parents' daily access to child-care centres?

Government officials have said "that is not decided yet" (Budget Estimates, p.94).

According to a media report, the Government has approved a $50 million software system, to be run by the Department of Family and Community Services, to track use of child-care down to the individual child ("Child ID cards in swipe at fraud", *Sydney Morning Herald*, 2 June 2006). The report says parents will be issued with swipe cards or PINs, needed to clock their children in and our of child-care centres.

Q: Why is there no proposal to prohibit anyone but DHS and DVA agencies from requesting (accepting) or demanding (requiring) the card for identification purposes?

Q: Has AUSTRAC been consulted about the likely impact on its regime of identification requirements, commonly known as the "100 points of ID" scheme, required when opening bank accounts?

Q: What has AUSTRAC advised about how many "points of ID" will be attributed to the so-called access card, given the Government is describing it as a "high quality proof of identity document"?

Q: Has the Privacy Impact Assessment specifically examined the likely increased incidence of data-matching and data-mining on customers in the private sector that will arise from this so-called access card, given the impending anti-money-laundering reforms, which will shortly introduce a new regime requiring customers of not only banks but lawyers, accountants, real estate agents and jewellers to identify themselves using the "100 points of ID" scheme?

Q: Given the impending anti-money-laundering reforms, what consultation has been done with the financial, legal, accounting, real estate and jewellery industries about the likely impacts of the so-called access card on their businesses?

Q: Does the $1.09 billion budget allocation include money for these businesses to install smartcard readers so that they can verify the validity of a so-called access card when it is presented to them as evidence of identity, as required under the impending anti-money-laundering reforms?

Q: Will the “low POI confidence flag” be visible on the face of a person’s card, or only found on the chip?

KPMG recommended that people who cannot meet the minimum standards of registration information should have a “low POI confidence flag” (KPMG Report, p.52).

If the “low POI confidence flag” is printed on the face of the card, it would likely lead to (or entrench) discrimination against already-disadvantaged people. In effect, some people would be flagged as second-class citizens.

However if this information is only held on the chip (as the KPMG Report recommends, p.52), how will third party users of the card be able to determine whether or not the card can be relied upon as ‘proof of identity’, unless they have a card reader? Requiring a card reader undermines the stated utility of the so-called Access Card as an all-purpose, simple and reliable photo ID card.

Q: How does the plan for a “low POI confidence flag” undermine other privacy promises?

The plan for a “low POI confidence flag”, to be held on the chip of cards issued to people who could not meet the minimum standards of registration information (KPMG Report, p.52), suggests that third party users of the card will need a card reader, to first test whether the Government is confident enough about each card holder’s identity to not issue a “low POI confidence flag”.

This has two implications: firstly, the alleged ‘privacy enhancing’ nature of the card, as a useful ‘proof of ID’ card with limited extraneous information on its face, is shown to be false – the extra information will simply be read from the chip instead; and secondly, the argument about the card number needing to be on the face (or back) of the card is also shown to be untrue.

The net result is that the Government is unable to deliver on one of its promises to deliver a simple ‘proof of ID’ card for people who suffer now from the lack of a photo ID card because they don’t have a driver’s licence. The card could only work as a ‘proof of ID’ card when read in conjunction with information stored on the chip, which opens the door for a far more privacy-invasive (and expensive) model of ID card than we have been promised to date.

This suggests to us that the Government should drop this proposed function of the card, and dramatically scale back the proposal to being a card that is only ever to be used to obtain DHS or DVA benefits.

# The ID number

Q: What is so different about the proposal for *this* ID number – most of us already have a driver's licence?

What is most significant and different about the proposed system is that there will be a personal number that is both unique and universal – meaning every person will have one, and the number will be unique to that person – that is included in a card carried by at least every adult.

Australians do not currently have assigned to them a single, universal and unique number on a government-issued document: drivers' licences and passports are unique but not universally held; current Medicare card numbers are universal but not unique, because they can cover more than one adult family member; tax file numbers are not printed on a government-issued document, and their use outside selected purposes is strictly prohibited. The so-called Access Card will involve a unique number for every person, and a unique card for every adult, with a number showing on the back of the card.

Q: What's wrong with having a unique and universal national ID number on a card?

The ID number becomes the key to unlock a myriad of records.

The creation of a single, unique and universal identification number means governments and businesses can not only identify people at the time of a transaction, but can also link their records with information about the same people collated from other organisations, and thus build up profiles of our activity.

The DHS ID number thus creates a single key, through which both governments and businesses can confidently index, link, track and profile our movements, transactions, and personal affairs, combining records in large scale and routine ways.

This poses privacy, physical security and identity security concerns.

Q: What is the estimated dollar value of identity fraud or theft likely to be generated by this project, as a result of creating a single universal and unique identifier for effectively all adult Australians?

Q: What does the Privacy Impact Assessment indicate are the privacy implications of creating a single universal and unique identifier for effectively all adult Australians?

Q: Has the Privacy Impact Assessment specifically examined the likely increased incidence of data-matching and data-mining on customers, across the public and private sectors, that will arise from placing a unique and universal ID number on the face (or back) of the card, given the need for card-holders to routinely present their card (and thus ID number) in order to identify themselves, or claim any concession-based discounts or rebates, to a vast range of government agencies and private businesses?

Q: What will prevent the use of the DHS ID number being used to link together the records generated from multiple requests for proof of ID?

Q: Has the Privacy Impact Assessment identified the following scenario: that the DHS ID number is used to track and link together records generated from a demand for photo ID each time a person boards a plane, mails a parcel overseas, visits a doctor, writes a cheque, fills a prescription, applies for social security benefits, rents a car, rents a house, buys some jewellery, seeks financial advice, seeks legal advice, or opens a bank account?

Q: Will any prohibition be placed on linking a person's DHS ID number to a business's customer records?

> The Government hasn't planned to legislate for prohibitions like this. When this scenario was put to Government officials giving evidence before the Senate, the best they could say was that this was "not in scope at the moment" (Budget Estimates, p.76).

Q: Will any prohibition be placed on linking a person's DHS ID number to other government records?

> We don't yet know. When this scenario was put to Government officials giving evidence before the Senate, the best they could say was that this was "not in scope at the moment" (Budget Estimates, p.76).
>
> At the moment it would depend on what privacy laws covered the other government departments. Some – not all - State and Territory government agencies are covered by privacy laws which prohibit the adoption of unique identifiers issued by the Commonwealth government.
>
> For example the NSW Government is introducing a smartcard ticketing program known as T-Card. The NSW Government has proposed that every T-Card issued to concession-card-holders will include details of their concession card or status on their T-Card. From 2010, the so-called Access Card would be the only means of proving that concession entitlement. The T-Card will thus record details of concession-holders' every movement on public transport, in an identifiable form, most likely including their DHS ID number. However the T-Card data will be held by a state-owned ticketing corporation that is exempt from both NSW and federal privacy laws.

Q: Has the Privacy Impact Assessment examined the likely link between the so-called access card and public transport ticketing programs?

Q: Given it is likely that the NSW Government's T-Card program will collect and use the DHS ID number (from the so-called access card) when issuing tickets to concession-card-holders in NSW, have the privacy implications of this use of the DHS ID number – that the physical movements of concession-holders on public transport can be linked to other information about their transactions - been considered with respect to the overall implications arising from the so-called access card?

# The Database

## *Database contents*

Q: What information about people will be held on the national population database (the "secure customer registration system", or SCRS)?

> First, the SCRS is proposed to have all the same information as is on the ID card's chip: "address, date of birth, concession status and details of any children or other dependents" (*Access card at a glance*, "What information will the access card hold?, DHS website). That must also mean your name, photograph and signature – and possibly includes the 'optional' information about emergency contacts and health information.
>
> Second, from other sources we have discovered that they also plan to store the biometric photo 'template', suitable for facial recognition purposes, as well as the digital photo itself (e.g. see KPMG Report, p.17).
>
> Third, there will be a unique number ("identifier") associated to each person – not just adults.
>
> Fourth, the SCRS will also contain information about customer relationships with each participating agency, such as a flag to indicate you are a current 'customer' of Medicare and CSA.
>
> And fifth, we know from answers given to Senators that the Government also intends to scan and keep copies of the documents you will have to provide, to obtain a card in the first place (Budget Estimates, pp.77, 95) – and that the stored copied will go into the SCRS (Taskforce Discussion Paper, p.12).

Q: Will the 'optional' emergency contacts and health information also be saved on the SCRS?

Q: Will people be able to nominate their preferred name (e.g. Bill / William, or maiden / married)?

Q: Will people be able to maintain different (but legitimate) names for different customer interactions across DHS / DVA agencies (e.g. Bill / William, or maiden / married)?

Q: Will the SCRS contain telephone numbers? (Will they be required? How will silent numbers be protected?)

Q: Will people be able to maintain different (but legitimate) addresses for different customer interactions across DHS / DVA agencies?

Q: Will people be required by law to supply an address?

Q: Will people be able to supply a post office box instead of their home address?

Q: Will people be able to suppress their home address so it is blocked from view of most or all readers of the database?

Q: Will people be required by law to maintain the accuracy of their address?

Q: Within what timeframe will people be required to notify each change of address?

Q: What will be the penalties for failure to notify a change of address?

Q: What data-matching with any other organisation, or against any other datasets, will be run, to identify cases of alleged failures to notify a change of address?

Q: Will the SCRS contain a copy of the photograph of the card-holder?

> Yes, the literature about the proposal on the DHS website says that lost cards can be reissued by post "because there is a registration photo" still in the SCRS (Fact Sheet (Access card at a glance), DHS website).
>
> However it also says that a biometric photograph "can be translated into a mathematical algorithm and used to test for similarity of appearance against the biometric photographs of other people…." (*Fact Sheet (Technology)*, DHS website). (Note however that the algorithm is not the set of numbers derived from a photograph, it is the method for doing the reduction. The proper term for the reduced biometric dataset is a "template".)
>
> Indeed the KPMG business case recommended: "It is proposed that the photo be capable of digital matching to prevent duplicate issuance of cards" (KPMG Report, p.16). This suggests that some storage of photographs is intended.
>
> One government official giving evidence to the Senate stated: "That photograph would be on the card, in the chip, and on the database" (Budget Estimates, p.75).
>
> A second official then stated: "at the point of capture when people register for the card that image will be able to be checked against the database of images and I will not be able to get two cards with my one face" (Budget Estimates, p.76).

Q: Will the SCRS contain a biometric template, describing the facial features of the card-holder (based on their digital photograph)?

Q: Why does the SCRS need both an actual photo, and the biometric template?

> The Consumer and Privacy Taskforce has suggested the reason for the SCRS storing the actual photograph, as well as the biometric template used for facial recognition purposes at the time of registration, is for a 'customer convenience' reason - so that lost or stolen cards can be replaced by mail, rather than requiring the person to come back in to repeat the registration process.
>
> However this 'customer convenience' would come at the expense of considerable privacy risks, and the Taskforce notes that "consumers might have more confidence in a system which is less convenient" (Taskforce Discussion Paper, p.20).

Q: Could the project objectives still be met without creating a national photographic database?

Q: What information will be stored on 'my' SCRS record for each of my children or listed dependents: e.g. will it include their card number (whether for issued or un-issued cards), SCRS ID number, photo, name/s, date of birth, gender, birth parents, relationship to me, whether a current/active relationship, and relationship start/expiry dates?

Q: How long will the dependent relationship data be stored on the SCRS, or in backups, archives or off line storage?

Q: What are the full range of dependent relationships to be recorded in the SCRS – e.g. spouse, de facto spouse, same sex partner, parent, non-custodial parent, step-parent, foster parent, carer …?

Q: Will the signature be stored on SCRS as an image (a digitised picture of a signature), or as a biometric?

Q: Why would the SCRS need to contain a scanned copy of my birth certificate and driver's licence?

> We understand the Government plans to scan documents and then check their veracity, before issuing a new Access Card – so the process is not necessarily 'on-the-spot'.
>
> However given the Government's separate initiative to fund the Document Verification Service, which aims to provide an online, real-time system for checking the veracity of evidence-of-identity documents such as birth certificates, immigration records, driver's licences and passports, we see no need for DHS or DVA to scan or copy most people's foundation documents.

Q: What security risks are posed by the proposal to let the SCRS contain a scanned copy of my birth certificate and driver's licence?

> In our view this presents a ludicrous security risk, as the database would contain not only the very documents needed to perpetrate identity theft elsewhere, but would in particular include each person's mother's maiden name (from birth certificates), which is one of things many banks and other businesses ask their customers as a so-called secret question/answer to establish one's identity when obtaining service over the telephone. Drivers' licences and passports can also include additional information about a person irrelevant to the purposes of DHS agencies or DVA, such as place of birth, or licence conditions such as the need to wear spectacles or use an alcohol-locking device.

## *Database access – DHS and DVA*

Q: Who will hold and manage the SCRS?

> The Government has stated that the SCRS will be "separate from DVA and Human Services agencies such as Medicare and Centrelink" (*Fact Sheet (Technology)*, DHS website).
>
> However when giving evidence before the Senate, one Government official claimed "the most likely location … is in one of the agencies", while a second added: "But completely separate" (Budget Estimates, pp.80, 81).
>
> Furthermore it became apparent that outsourcing the SCRS to a private firm "has not been ruled in or out" (Budget Estimates, p.81).

Q: Who will have access to the data held in the SCRS?

> The Government has stated that access to the SCRS will be limited to "authorised people" (*Access card at a glance*, "What information will the access card hold?", DHS website).
>
> This is of course a non-answer, intended to reassure without actually promising any protection whatsoever. (As if a Government would ever answer that it would enable access to "unauthorised people"!) The question remains: who will be 'authorised'?

Q: Which DVA and DHS agencies will have access to the SCRS?

Q: If the Child Support Agency (part of the DHS) will have access to the SCRS, why is this not mentioned in the Government's literature?

Q: How will agencies have access to the SCRS? (e.g. open, online access? limited access to individual records on request?)

> The Government has stated that the SCRS will ensure that information is "kept up to date across Medicare, Centrelink and the Department of Veterans' Affairs" (*Fact Sheet (Technology)*, DHS website).
>
> Government officials giving evidence before the Senate first suggested that "any staff member of any agency who needed to see that information would see only that information" (Budget Estimates, p.74). However this was later contradicted: "they will be able to read the card to confirm the photograph but they would not be able to access the secure customer registration system" (Budget Estimates, p.80).

Q: Approximately how many different people will have access to the SCRS across DVA and DHS?

Q: What strategy is there to make the people who have authorised access to create, add to or amend records in the SCRS less 'error-prone' than existing DHS / DVA staff?

## *Database access – card-holders*

Q: How will people be able to see and correct their own records held in the SCRS?

> The Government has stated that the people will be able to view and update their information by accessing the SCRS online (Budget Estimates, p.77).
>
> However online service delivery using a smartcard depends on the user having a smartcard reader attached to their PC – which will only slowly become commonplace. Without a smartcard reader, online service delivery depends on login/password combination, which is insecure and subject to 'phishing' attacks.

Q: How will online access to the SCRS work – with smartcard readers, and/or login/passwords?

Q: How will people identify themselves over the internet to obtain access to their own records, without exposing themselves to identity fraud or theft, if they don't have their own smartcard reader?

Q: What is the estimated dollar value of identity fraud or theft likely to be generated by this project, as a result of allowing individuals' online access to the SCRS, ripe for targeting by phishing and similar attacks to obtain people's passwords?

Q: How else might people be able to see or update their records?

> Government officials giving evidence before the Senate have said that most likely people would seek to change their information (such as notify a change of address) over the telephone, using the 'secret questions and answers' (SQA) technique that is used now by Centrelink (Budget Estimates, p.81).
>
> Yet the SQA technique was criticised by KPMG as not providing the two-factor authentication and non-repudiation now required under the Australian Government's Authentication Framework (KPMG Report, p.6).
>
> KPMG anticipates that even with the card, the "majority of service settings will be face-to-face" (KPMG Report, p.20). Government officials have also mentioned the ability to use a computer 'kiosk', located within a Centrelink office (Budget Estimates, p.81).

## *Database access – third parties*

Q: Other than the card-holder themselves, and DVA and DHS agencies, what other people or organisations will be "authorised" to have access to the SCRS?

Q: How will third party access be made available, and in what circumstances?

Q: Will all information on the SCRS be made available, or will components be 'siloed'?

Q: Will state and/or federal police forces, or security agencies such as ASIO, have access? In what circumstances?

> When asked about police and ASIO access to the SCRS, Government officials giving evidence before the Senate said "Nothing will change in terms of the powers of those people" (Budget Estimates, p.75). They also said that police and security force access had not been considered in the Privacy Impact Assessment prepared as part of the business case.
>
> However later, when asked about the possibility of matching photographs taken from CCTV footage as against the photos held in the SCRS, the official admitted that while there were "no plans at this stage to link the two", they had been speaking to AGIMO about the national standards for CCTV (Budget Estimates, pp.79, 80).

Q: Will the Tax Office have access? In what circumstances?

Q: Will DIMIA have access? In what circumstances?

Q: Will the Australian Bureau of Statistics have access? In what circumstances?

Q: Will researchers have access? In what circumstances?

## *Database uses – data-matching*

Q: Outside the DVA and DHS agencies, what other people or organisations will be allowed to conduct or participate in data- matching, data-mining or data-cleansing as against the SCRS?

Q: What other sources (people, organisations or datasets) will be used by the holder of the SCRS to conduct data-matching, data-mining or data-cleansing?

Q: What prohibition will there be on linking a person's data to data about their family members?

Q: What prohibition will there be on linking a person's data to census data?

Q: What prohibition will there be on linking a person's data to data from the electoral roll, the Integrated Public Number Database (which includes silent numbers), or driver's licence databases?

Q: What prohibition will there be on linking a person's data to fingerprints, DNA and/or criminal records held by CrimTrac or police forces?

Q: Will facial recognition technology be used to match people photographed on CCTV cameras to identify them from the centralised database?

> When asked about the possibility of matching photographs taken from CCTV footage as against the photos held in the SCRS, a Government official admitted that while there were "no plans at this stage to link the two", they had been speaking to AGIMO about the national standards for CCTV (Budget Estimates, pp.79, 80).

## *Database security*

Q: What security arrangements will there be around the database?

> The Government has only said "it will be a lot more secure than any other system that we have" (Budget Estimates, p.80).
>
> The Consumer and Privacy Taskforce has only noted that the Government "*may* put technological arrangements in place to prevent unauthorised access" (emphasis added) (Taskforce Discussion Paper, p.10).

Q: What security ranking will be applied to the data held on the SCRS, under the Information Security requirements of the Commonwealth Protective Security Manual – e.g. "protected", "highly protected", "secret" or "top secret"?

Q: What strategy is there to make the people who have authorised access to the SCRS more 'corruption-proof' than existing DHS / DVA staff?

None that we can find. The Minister has simply said that "The same penalties, including gaol terms, that apply to Human Services Agency staff for inappropriately accessing a database will still apply and may even be increased" (Joe Hockey speech to the AMA National Conference, 27 May 2006).

We believe the SCRS will not be any more secure, or free from corruption, than any other database.

Q: When was the last time a public servant from DHS accessed or disclosed personal information inappropriately from a client database?

According to the Opposition, a recent internal audit of the Child Support Agency, obtained under Freedom of Information, found 405 privacy breaches over nine months, of which 69 involved sensitive information being disclosed about people to their ex-spouses. The Opposition has also claimed that the breaches placed mothers and children at risk, and in two cases the Government had to pay to relocate families as a result. This internal audit report does not appear to be publicly available ("Privacy disregarded by Child Support Agency", Media release by Kelvin Thompson, Shadow Minister for Human Services, 2 June 2006).

Q: When was the last time a public servant from DHS lost their job for accessing or disclosing personal information inappropriately from a client database?

Q: When was the last time a public servant from DHS was fined for accessing or disclosing personal information inappropriately from a client database?

Q: When was the last time a public servant from DHS went to gaol for accessing or disclosing personal information inappropriately from a client database?

Q: What screening process will be applied to the staff who will have access to the SCRS?

Q: Will every user of the SCRS be given a unique log-in identity?

Q: Will card-holders be able to specify certain users to be barred from accessing their records (e.g. an estranged family member who works in Centrelink)?

Q: Will there be an audit trial or 'log' of every amendment to a record?

Q: Will there be an audit trial or 'log' of every time a record is *viewed* or printed with or without amendment?

Q: Will the Government commit to a "database breach notification" legal requirement, as many States in the USA are now adopting, so that people at risk of identity fraud or identity theft because of a security breach of the SCRS database can be warned and can take preventative action?

The Acting Head of the Office of Access Card has said "If anything goes wrong and we know about it, obviously we will inform the customer" (Budget Estimates, p.78).

Q: How many staff will be employed to assist people with re-establishing their identity in the event of identity fraud or identity theft, arising from a security breach of the SCRS database?

Q: What is the estimated dollar value of identity fraud or theft likely to be generated by this project, as a result of creating a single 'honey-pot' database containing the name, current address, date of birth etc for effectively every adult in Australia, ripe for targeting by hackers or organised criminals?

# Governance

## *Loopholes in the law*

Q: Is the federal Privacy Act strong enough to cope with the implications of this proposal?

Not even close.

Not all third party users of the so-called access card, the ID number and/or the data in the SCRS will be covered by privacy laws. Exempt bodies include:

- political parties
- media organisations
- small businesses
- large businesses in relation to their employee records
- government agencies in Qld, SA and WA
- police and state-owned corporations in NSW (including significant holders of personal information such as utilities and public transport / ticketing agencies)

Numerous reviews have already found further loopholes and leakage points in both State/Territory and federal privacy laws. Another, more comprehensive review of our system of privacy laws is now underway at the Australian Law Reform Commission, at the request of the federal Government, which is due to report in 2008.

It is worth remembering that the federal Privacy Act was drafted in 1988, immediately after the 'Australia Card' proposal for a national ID card was withdrawn. The challenges posed by such a scheme were therefore not contemplated in 1988. In fact it was opposite: the federal Privacy Act was drafted to suit an environment in which there would be *no* such proposal.

Q: Given the concerns that our system of privacy laws in Australia is not adequate to deal with new technological challenges, why does the Government not act first to plug the loopholes and leakage points, or at least wait for the results of the ALRC review, before introducing the highly risky and highly invasive so-called access card?

Q: What legislation is proposed to limit function creep, data creep and access creep?

Q: Given the possibility of function creep, data creep and access creep, how will decisions be made about future 'bids' for access, both to the card itself and to information on the SCRS, both within and outside the current proposed agencies, objectives and data content limits?

## *The consumer and privacy taskforce*

Q: Was the consumer and privacy taskforce recommended by KPMG?

No. KPMG recommended a wider stakeholder advisory body, whose role it would be to provide a single point of coordinate stakeholder advice to the Minister, and provide advice to government to ensure business rules and detailed design reflect consideration of the privacy issues raised (KPMG Report, p.31).

Q: What is the purpose of the taskforce?

The taskforce has been given no written terms of reference. This makes its purpose vague, and open to interpretation.

The Office of Access Card website says the taskforce is "to address consumer and privacy issues related to development of the (access card) … and "provide independent advice to the Minister on consumer and privacy issues".

Government officials have also suggested the taskforce "to develop detailed advice to the government on operational issues and on how implementation risks can be managed" (Budget Estimates, p.76).

The taskforce itself describes its role as "to facilitate a process of community consultation about the issues raised by the Government's access card and to open up additional lines of input to the Government's final decision making" (Taskforce Discussion Paper, p.1).

The taskforce has expressly excluded itself from commenting on "the analysis presented by Government and its other advisers about either the cost of establishing the proposed scheme, or the financial benefits or savings expected to revenue which are expected to accrue" (Taskforce Discussion Paper, p.18).

Q: What is the scope of issues the taskforce will examine?

The Office of Access Card website states: "The primary focus of the Taskforce will be to address the tension between meeting consumer demand for increased Access Card functionality and any concerns that consumers may have about data protection and privacy issues".

This suggests that the Government expects the only tension to be reviewed will relate to any *additional* functionality, not the proposal as it exists now.

The taskforce itself appears to have also set some limitations in terms of its willingness to examine issues arising from the proposal. While stating that "a robust case … must be made out" by the Government for collecting new information not currently held by any DHS or DVS agency (specifically, biometric photographs and digitised signatures), no mention is made of the privacy and data security concerns that also arise from the proposal to combine, use, share or store existing data in new ways (Taskforce Discussion Paper, p.19).

Q: What does the Minister mean when he suggests that consumer demands and privacy protection might be at odds – don't "consumers" want their privacy protected too?

Privacy protection is of course one of the many concerns that people, or "consumers", will have. We reject the notion that somehow consumer concerns and privacy concerns are at odds.

However there is a conflict between the arbitrarily specified "convenience" of having everything saved both on your card's chip and on the SCRS database (so that a lost card can be instantly replicated, including photo and signature, just from the SCRS database), and the fundamental data security and privacy hazards that this central duplication of such a rich dataset of personal information inevitably creates.

Ultimately the value in the SCRS is for the Government, not "consumer convenience" – the purpose of the SCRS is to enable mass population surveillance, data linkages and data mining.

Q: What will be the work of the taskforce?

The Minister has described the role of the taskforce as "to consult on consumer and privacy issues" (Joe Hockey press release, 28 June 2006).

Government officials have suggested the taskforce would "take on board the concerns of consumers and privacy advocates in relation to this project to feed them back to the deputy secretary and directly to the minister so that we can make any necessary adjustments" (Budget Estimates, p.70).

Specific work tasks suggested by Government officials as to be dealt with by the taskforce include determining if any changes are needed to policy as a result of the Privacy Impact Assessment previously done (Budget Estimates, p.66); and what limits should be put on the card's use by third parties seeking 'proof of ID' (p.76).

Q: Is the taskforce independent of the Government?

The Minister for Human Services, Joe Hockey, has described the taskforce as "independent" (Joe Hockey press release, 6 June 2006).

However Government officials denied it was "an independent body", instead describing the taskforce as "a task and consultative dimension of the implementation group" (Budget Estimates, p.72).

Three of the four taskforce members are contracted to, and paid by, the Department of Human Services. The fourth is an employee and direct representative of the Department.

Q: Can the Minister sack the taskforce members if he disagrees with their advice?

Yes, via his Department.

The terms of appointment of the taskforce members are based on a standard labour hire contract for a specified time, subject to renewal.

Unlike statutory independent positions which require proof of incapacity or corruption and only allow removal by a third party such as the Governor General, we understand the taskforce members' employment contract allows either party to terminate the contract at any time. The Department of Human Services is the relevant party which can terminate the services of one or more taskforce members at any time.

Q: What is the accountability of the taskforce?

The taskforce chair, Allen Fels, reports directly to the Minister for Human Services, Joe Hockey.

Q: Is the taskforce neutral or in favour of the so-called access card going ahead?

Government officials have said the taskforce is part of the "implementation group" within the Department of Human Services (Budget Estimates, p.72).

The Chair of the taskforce, Allen Fels, has said: "I accepted the appointment because I believe the access card has the potential to significantly benefit Australians by cutting red tape for families and business as well as making access to government services simpler. Of course this all needs to be balanced with appropriately defined privacy and security protections" (Joe Hockey media release, 24 May 2006)

Allen Fels has also said: “I guarantee that community issues will be fully considered during the development of an access card system” (Joe Hockey media release, 7 June 2006).

Q: Who is on the taskforce?

The taskforce chair is Professor Allen Fels, whose appointment extends to roughly one day per week. Full-time members are Chris Puplick (former NSW Privacy Commissioner), and John Wood (for Commonwealth Deputy Ombudsman). The fourth member, Ben Battisson, is an employee and representative of the Department of Human Services.

Q: Were the taskforce positions advertised or subject to expressions of interest?

No.

Q: Will the taskforce be ‘staffed’ with a secretariat?

The members of the taskforce appear to be it, although the taskforce has said that additional members may be appointed (Taskforce Discussion Paper, p.4).

Q: What is the budget for the taskforce?

They don’t have a budget appropriation. Requests to expend money must apparently be made to the Minister.

Q: Is the taskforce’s budget part of the $47.3m “communications strategy” budget, or is it part of the design budget?

Q: What will be the taskforce’s budget to seek independent advice?

None, unless they can first convince the Minister to provide them with the money.

However the taskforce appears to be planning to do so: “The Taskforce will be drawing upon other specialist assistance from time to time by commissioning the production of papers on various technical matters to assist in its deliberations” (Taskforce Discussion Paper, p.4).

Q: Will the taskforce have the authority to demand documents from the Government?

No. The taskforce has no statutory existence, and therefore no powers at all.

Q: Will the taskforce have the authority to publish documents from the Government?

No. The taskforce has no statutory existence, and therefore no legal authority at all. Any publication of documents provided to them by the Government could be in breach of the law of confidence.

However the Chair of the taskforce has indicated he is willing to speak out publicly if necessary: “As an independent advisor, I can provide an objective perspective to the Minister and his department, and to the community, as we address the issues and work through them,' Professor Fels said” (Joe Hockey media release, 24 May 2006).

Q: Will the taskforce make public all its recommendations and reports to the Government?

It has not specifically promised to do so, although it has said that it "intends to conduct its proceedings in as open and public a fashion as possible" (Taskforce Discussion Paper, p.4).

Q: Are the taskforce's consultations being conducted in an independent fashion?

It would appear that a representative of the Department of Human Services is sitting in on each consultation meeting. This creates the perception that taskforce members are being 'minded'. There is a risk that genuine and independent debate is being stifled as a result, whether intentionally or not.

Q: Will the taskforce have the authority, resources or technical backup to cancel the project, or make it conditional on adequate scope, technical, legal and administrative protections?

No. The taskforce has no statutory existence, and therefore no legal authority at all. The best they can do is recommend to the Minister that he change or cancel his own project.

The taskforce itself ahs noted that "all final decisions will remain with the responsible Minister and the Government" (Taskforce Discussion Paper, p.5).

The Minister has said of Professor Fels, "I obviously listen to everything that he says and take heed of certain things" (Parliamentary debate on *Appropriation Bill (No. 1) 2006-2007*, 19 June 2006).

Given the lack of terms of reference, formal powers or statutory or financial independence, and the existence of a Departmental representative on the taskforce, we are concerned that the Government sees the purpose of the taskforce as just to smooth the passage of the project, and lull Australians into a false sense of security, rather than genuinely make input into the design process or speak on behalf of the public interest.

## *Assessing the privacy implications*

Q: What assessment was done by KPMG to consider the privacy implications of the project, as part of its development of the 'business case' for the Government?

Very little it would seem. Privacy is described as a concern to be "dealt with", as a set of "issues which need to be managed", as concerns to be addressed at "the implementation stage and thereafter", or as a subject of "reassurance" as part of the communications strategy" - rather than actually *resolved*, by way of building-in privacy protections during the planning and design stages (KPMG Report, pp.3, 13, 28, 32).

It is very difficult to have confidence in the likelihood of privacy "add-ons" being effective, once the Government has committed to a specific technology model.

Under the heading "The right balance", the KPMG Report only mentions how the project could be privacy enhancing (streamlining the process of amending or updating commonly-held information such as change of address), without mentioning its potential to be privacy invasive (KPMG Report, p.12; see also p.28).

Q: What assessment has been done by the Government to consider the privacy implications of the project?

A Privacy Impact Assessment (PIA) on the proposal was commissioned from Clayton Utz by the Department in late 2005, and additional advice was provided by a private privacy consultant.

Q: What did the Privacy Impact Assessment say about the proposal?

We don't know, because the Minister won't release the document.

Q: What did the Privacy Impact Assessment cover in its scope?

We don't know, because the Minister won't release the document. However Government officials have said that the PIA did not review law enforcement bodies' access to the SCRS database (Budget Estimates, p.75). They were not sure whether or not the PIA looked at the issue of using the biometric photograph to match against photographs taken of suspects by CCTV cameras (Budget Estimates, p.85).

Q: What recommendations did the Privacy Impact Assessment make about the proposal?

Government officials have suggested that no recommendations were made at all (Budget Estimates, pp.64, 66). We find this difficult to believe, especially as one of the authors has been quoted as saying one of his recommendations was that the PIA be made public ("Smartcard contracts blow budgets", *The Australian*, 30 May 2006).

Q: Why was the original Privacy Impact Assessment not released and open for public consultation before Cabinet approved the project and the budget was approved?

One Government official suggested that the PIA was not released because "it is still a work in progress, so it is not complete" (Budget Estimates, p.64). However he was quickly contradicted by another Government official, who said the PIA had been finalised at the same time as the KPMG Report was finalised, as they had "proceeded in parallel … I believe the work is complete, yes" (Budget Estimates, p.65).

Q: Why won't the Minister release the Privacy Impact Assessment now?

The Minister Joe Hockey made a commitment to the Australian Privacy Foundation on 9 May 2006 that he would publish the PIA shortly. However at a later press conference on 24 May 2006 he said he would not release the PIA because it was now "redundant".

Government officials the following day suggested that although it was "not necessarily out of date", the PIA had not been released because it was "not at the level of detail … to be considered alongside a detailed design specification for how the access card will operate" (Budget Estimates, p.69). Officials also suggested the PIA had not been released because it was Cabinet-in-confidence (Budget Estimates, p.64).

Q: Was the Privacy Impact Assessment prepared concurrently with the KPMG business case (i.e. was it reviewing the same model as KPMG was)?

Yes: "the initial privacy impact assessment and the development of the business case have … proceeded in parallel with one another" (Budget Estimates, p.60).

So if the PIA is now 'redundant' as claimed by the Minister, then surely the KPMG report is also redundant – yet the Minister continues to quote the KPMG financial estimates to justify this project, without releasing the full details.

Q: Were any features of the proposal changed in response to recommendations in the PIA, prior to taking the proposal to Cabinet?

> The Government saw the PIA as "an input into the policy consideration processes by government" (Budget Estimates, p.65); yet later the same official said "there were no changes to the business model following the completion of the initial privacy impact assessment" (Budget Estimates, p.68).
>
> Another official said "any changes to the policy as a consequence of the privacy impact assessment" is yet to be done, and is instead to be the work of the taskforce (Budget Estimates, p.66).
>
> Yet the Minister contradicted this position, claiming of the PIA that "the advice received from Clayton Utz and others was essentially made redundant because the nature of the project changed according to the decision of cabinet" (Parliamentary debate on *Appropriation Bill (No. 1) 2006-2007*, 19 June 2006).

Q: What features of the proposal have changed since the original PIA was prepared?

Q: What was the point of commissioning a Privacy Impact Assessment if it was not going to impact on the system design, or be publicly released as part of the consultation process?

> We suspect the PIA *did* make recommendations, and probably said things the Government didn't expect to hear, and consequently doesn't want anyone else to hear – such as that the project ran the risk of becoming a defacto national ID card.
>
> This was hinted at by Government officials, who noted that "There were certainly concerns about whether this is an ID card or not … that was the concern that was highlighted in the initial privacy impact assessment" – but that since then the "ID card issue has been resolved; it is not an ID card" (Budget Estimates, pp.64, 69).

Q: Will there be further PIAs on the proposal, each time it changes? Will they be prepared independently? Will they be released? Will they feed into the design process?

> Government officials have indicated that a "more detailed privacy impact assessment will almost certainly need to be done once the detailed specifications of the access card model have been developed", and "once we know exactly how it is going to work" (Budget Estimates, pp.60, 67).
>
> However the Minister has simply said that "Professor Fels is a living, breathing privacy impact assessment" (Parliamentary debate on *Appropriation Bill (No. 1) 2006-2007*, 19 June 2006).
>
> One project 'risk' identified by KPMG is that legitimate privacy concerns will not be addressed "at both the implementation stage and thereafter" (KPMG Report, p.13).

Q: Is the Government utilising PIAs the way they should be?

> We don't believe so.
>
> What is of great concern to us is there appears to be no recognition, either by KPMG or the Government, that privacy considerations need to be built-in at the planning and design stages of the project, not just 'managed' through a 'communications strategy' at the implementation stage, when it is too late to change the design specifications.
>
> Furthermore, PIAs should be publicly released, along with the draft design documents, to give the public an opportunity to make fully informed judgments about what level of privacy protection they find acceptable.

## *Assessing the costs and financial savings*

Q: Are the costs and financial savings estimated by KPMG fixed in stone?

> No; "things that are in the KPMG report will change as we get a lead adviser on board and we make some specific decisions about exactly what it is that we are going to be doing" (Budget Estimates, p.60).

Q: What are the detailed costings?

> We don't know. They are in Volume 2 of the KPMG Report, which has not been released.

Q: What comparisons were done with overseas experience, to test the assumptions and estimates of cost, time and benefits?

> KPMG "sought comparable overseas examples to validate our implementation timeframe but found no uniform models for implementation" (KPMG Report, p.29).

Q: Will the Consumer and Privacy Taskforce be able to provide independent review of the proposal's costings?

> No. The taskforce has expressly excluded itself from commenting on "the analysis presented by Government and its other advisers about either the cost of establishing the proposed scheme, or the financial benefits or savings expected to revenue which are expected to accrue" (Taskforce Discussion Paper, p.18).

## *Assessing the alternatives*

Q: Will the original instructions to KPMG be released?

Q: Will any subsequent instructions to KPMG be released?

Q: Was KPMG tasked with reviewing the business case for one pre-determined 'model', or was it asked to review multiple options and recommend one?

> "KPMG was asked to prepare a business case for the introduction of a Health and Social Services smart card initiative" (KPMG Report, p.1).
>
> KPMG also identified some alternative models, which it quickly dismissed, such as remaining with the status quo, upgrading the Medicare card from magnetic stripe to smartcard but not touching the other 16 cards, or keeping the existing cards as is but changing the customer registration processes (KPMG Report, pp.23-24).
>
> However they did not appear to consider the costs, benefits or privacy implications of the option of introducing a single DVA and DHS welfare benefits smartcard, and *separately* introducing a Medicare smartcard.

Q: Has the Government estimated the costs, benefits and privacy implications of the option of just introducing a single DVA and DHS welfare benefits (but not Medicare) smartcard?

Q: Has the Government estimated the costs, benefits and privacy implications of the option of introducing a single DVA and DHS welfare benefits smartcard, and *separately* introducing a Medicare smartcard, to maintain separation between health and welfare information?

## *On-going governance, and managing project risks*

Q: What recommendations did KPMG make about project risks, and how best to deal with them?

KPMG identified several "threats and weaknesses of implementing the HSS initiative", including:

- "governance arrangements which do not provide clear points of accountability"
- the failure to address "legitimate privacy concerns"
- function creep: "continual customisation of the card" and "adding new functions without a proper value proposition"
- "overstating the benefits" and ignoring other opportunities for service reform, and
- a "history of unrealised returns and benefits in many large scale projects of this kind" (KPMG Report, p.13).

To respond to "these inherent weaknesses in a project of this scale", KPMG then suggested a set of governance arrangements (KPMG Report, p.14).

They recommended the establishment of a single implementation unit within DHS, but with a Board including the Federal Privacy Commissioner, the CEOs of the Medicare and Centrelink, and the Secretaries of DHS and a number of other federal government agencies (KPMG Report, p.31).

KPMG also recommended the establishment of a wider stakeholder advisory body, with an independent chair, whose role it would be to provide a single point of coordinate stakeholder advice to the Minister, and provide advice to government to ensure business rules and detailed design reflect consideration of the privacy issues raised (KPMG Report, p.31).

Q: What recommendations did the DHS smartcard project taskforce make about project risks, and how best to deal with them?

The Department of Human Services smartcard project taskforce presented the Minister with a range of governance options, but recommended that the Office of Access Card should be an independent statutory agency (Budget Estimates, p.91).

Q: Which of these recommendations did the Minister accept?

On 4 May 2006 the Minister rejected the recommendation about creating an independent statutory agency; he decided to create the Office of Access Card as a unit within his Department.

The Minister also rejected KPMG's recommendations for a Board (including the Federal Privacy Commissioner) to oversight the implementation unit. Instead the Office of Access Card would appear to report directly to the Minister.

The recommendation for a stakeholder advisory body was also rejected, in favour of the smaller consumer and privacy taskforce.

After the Minister made these decisions, the two most senior staff from the smartcard project taskforce resigned, with the taskforce head James Kelaher making public his protest about the Minister's decisions (Budget Estimates, p.91).

## *Assessing public support*

Q: What consultation was done on the proposal as part of developing the 'business case'?

KPMG claimed to have "consulted extensively in the preparation of (the) business case". Yet the footnote to this comment only refers to " meetings with a range of financial industry representatives, including major banks and credit card companies" (KPMG Report, p.8). The list of people or organisations consulted has been deleted from their Report.

The KPMG Report also suggests that it consulted with privacy advocates: "KPMG has noted and considered the comments made by privacy advocates during consultations" (KPMG Report, p.18).

The Government also claimed that KPMG "did an extensive range of stakeholder consultations … (which) included detailed discussions with Medicare, Centrelink and the department in building up the business case" (Budget Estimates, p.56).

However while the Australian Privacy Foundation and other privacy and consumer groups were consulted about an earlier set of models by the Department of Human Services in mid 2005, they were not consulted by KPMG, or the Department, on the proposal for a card that would be *compulsory* to access any Medicare or social security benefits.

Indeed government officials later admitted that there was no "broad-ranging consultation" with privacy or consumer groups "in the development of the business case … That is a bit of work that remains ahead of us" (Budget Estimates, p.94).

We suggest it is entirely disingenuous and misleading for KPMG to have written a report which leaves readers with the incorrect impression that privacy advocates were consulted by KPMG on the business case it was preparing.

Q: Will the Government agree to a referendum on the introduction of the so-called access card?

In 1987, when he was leader of the opposition, John Howard demanded a referendum be conducted on the 'Australia Card' proposal, to test the claims of broad public support for the proposal.

We demand one now.