NSWCCL
New South Wales Council for Civil Liberties

New South Wales Council for Civil Liberties Inc
149 St Johns Road
Glebe NSW 2037
Australia
www.nswccl.org.au

Ph 61 2 9660 7582
Fax 61 2 9566 4162
Email office@nswccl.org.au
DX 1111 Sydney

Correspondence to:
PO Box 201
Glebe NSW 2037
Australia

24 July 2006

Allan Fels
Char, Access Card Consumer and Privacy Taskforce
PO Box 3959
Manuka ACT 2603

By email: a.fels@humanservices.gov.au

Dear Sir,

Re: 'Access Card'

1. The NSW Council for Civil Liberties (CCL) thanks the Access Card Consumer and Privacy Taskforce (the Taskforce) for the opportunity to make this submission.

2. CCL is deeply concerned with the government's proposed introduction of the new 'Access Card.' The proposal, as it now stands, explicitly introduces a new national identification card. In fact, what we know of the current proposal makes it even more problematic from a civil liberties perspective than the 'Australia Card' proposal of the 1980's. Simply put, without a legislative framework constraining the functions, use, and access to the card and the new information databases that it will spawn, the new card is in effect, if not in name, a national ID Card.

3. Ultimately, CCL is not only concerned by what the public has been told about the proposal, but also equally concerned by the details and potential problems that the government has undemocratically withheld from the public. Even with serious legislative constraints, which this paper will suggest are at the very least necessary, CCL opposes the introduction of a system that will enable the government and potentially private businesses to track and profile the everyday movements of Australians.

4. The 'Access Card' will create an unprecedented identity database in Australia. While such grand invasions of privacy have come to be tolerated over time in some European and totalitarian nations, the Australian democratic tradition has been strongly and continuously opposed to such Orwellian proposals.

The 'Access Card' goes beyond previous proposals for a national identification card.

5. The 'Access Card' shares many of the same components as the repeatedly failed 'Australia Card' proposal.

6. Both the 'Access Card' and the 'Australia Card' involve assigning a unique ID number to virtually every Australian. While proponents of the card flaunt that unlike the 'Australia Card' this new card will not be mandatory, in reality the vast majority the Australian adult population will be forced to acquire the card at some point in their lives. This submission discusses the involuntary nature of the card in more detail below.

7. Like the proposed 'Australia Card,' and other national identification cards in use around the world, each 'Access Card' will contain a photograph of the card-carrying adult along with that person's unique identification number and signature. In addition to the photograph and unique numerical identifier, key components of any national identification card scheme, the government has itself marketed the 'Access Card' as a new form of highly reliable "all-purpose" proof of identification.

8. Both cards create a national population database with names, photos, dates of birth, ID numbers, and addresses of every adult along with a corresponding listing of their dependents (who, it appears, will also be given a number to be activated when they obtain a card of their own at some later date).

9. CCL also notes that like the 'Australia Card' the new 'Access Card' will be compulsory for access to Medicare and any other government entitlements. While not required by law to carry the card at all times (one would not have been required to carry the 'Australia Card' at all times either), the various functions and potential functions of the card make it unlikely that Australians will keep the card in a safe place and at home. Because the card is being marketed as an "all-purpose" proof of identification card, it will likely be awarded a higher identification point value, potentially replacing the driver's license as the identification of choice.

10. The 'Access Card,' however, goes beyond the 'Australia Card' in that it will contain extra information on the new smart chip, will replace all concessions cards, and will create a database containing biometric photographs of every person, a technology not available at the time of the 'Australia Card' proposal. The additional benefits being hyped by the government all represent storage of larger amounts of private information than proponents of the 'Australia Card' ever envisioned.

11. It is also worth noting that when the Tax File Number was introduced safeguards were put in place so as to prevent the number becoming a national ID number.

Such safeguards do not exist in any form with the current proposal. And, unlike the current Medicare Card number, the new proposal will introduce a unique number to the every individual as opposed to a family. The new proposal is not simply a technological upgrade of an aging system, but the groundwork of a new national ID system.

The 'Access Card' is not voluntary.

12. The Taskforce has already acknowledged that "at some stage, almost every Australian is likely to need an access card."[1]

13. Between Medicare services, concession related benefits, Centrelink entitlements, PSB safety net access, and identification purposes only the very rich and privacy conscious will be able to survive without the card.

14. Even if a significant minority of people become accustomed to using their 'Access Cards' as their primary means of identification, without legislation prohibiting government officials, police, and private parties from requiring to see the card (or requiring them to accept another form of identification instead of the card), the card will quickly become mandatory. As the Taskforce cited in its initial Discussion Paper, the Drivers License is a good example of how a card designed specifically to identify certified drivers became the standard form of identification.

15. Currently the government has not proposed any legislation to limit who may ask to see your card. The government has also not proposed any legislation requiring government officials not authorized to distribute entitlements (police for example) or members of the public at large "landlord for example" to accept alternative forms of identification.

The system is being designed to specifically facilitate function creep.

16. The government has not committed to legislation that would limit the functions of the new card.

17. The government has not proposed a framework whereby any new additions would have to be approved by both the House and the Senate.

18. The government has not proposed an administrative framework that would mandate public debate and consultation prior to any additional functions are approved for the 'Access Card.'

19. The government has not proposed to re-examine the Commonwealth's current privacy legislation in the wake this new identification scheme and photographic

[1] "Discussion Paper Number 1: The Australian Government Health and Social Services Access Card." Access Card Consumer and Privacy Taskforce, p. 19.

database that goes well beyond anything currently existing in Australia. This review of existing privacy legislation is necessary because the Privacy Act was created in the wake of the 'Australia Card's' defeat. Members of parliament did not design the act with an eye towards a comprehensive national identification scheme like the current proposal for the 'Access Card' that will likely surpass the defunct 'Australia Card' proposal in terms its invasion of privacy.

20. While the government has stated that the new database will not act as a Repository of Electronic Health, the Minister has stated that there may be room for discussion at a later date.[2]

21. Additionally, while the government has stated that it has yet to formulate plans to link the biometric photographic database with CCTV camera footage, they have acknowledged that they been speaking to AGIMO about the national standards for CCTV.[3]

22. The Taskforce has already identified function creep as an area of concern in need of community consultation, and cited the United States experience with the Social Security Card as an example:

    "over a period of time since its introduction in 1938 and usually without public debate or Congressional approval - grew from being a mere social security identifier into a multi-purpose identifier used well beyond anything for which it was intended originally."[4]

23. Unlike the Social Security Card, however, the new 'Access Card' is poised to become, and is being marketed as, a new "all-purpose" high quality identifier in addition to its function as the means to obtaining entitlements and concessions. The Social Security card has never had this everyday functionality. Compare opening a bank account, where the number is necessary in the United States, to getting concessions on public transport, where the number and the card would be compulsory in Australia. Moreover, the Social Security Card does not have a picture on the front corresponding to the unique identifier and cannot, therefore, be used as a form of everyday ID. Social Security Cards and the information contained thereon are guarded much more cautiously than the 'Access Card' will be in Australia.

24. Thus far the only statements from the government as to express functional limits on the card come from the Budget Estimates Hearings when government officials noted that any change in function would merely have to be "either requested by consumers or a decision of government."

---

[2] Joe Hockey speech to AMA National Conference, 27 May 2006.

[3] Commonwealth of Australia, Senate, Finance and Public Administration Legislation Committee, Budget Estimates, Canberra, Proof Committee Hansard, 25 May 2006. Evidence given by Mr. Geoff Leeper, Acting Secretary, Department of Human Services, and Mr. Graham Bashford, Acting Head, Office of the Access Card, pp. 79, 80

[4] Taskforce Discussion Paper.

25. Aside from refusing to call the 'Access Card' anything that might resemble a national identification card, there are no functional limits as yet to the government's current proposal.

The photo on the front of the card, stored in the chip, and on the SCRS database raises numerous concerns of significance for Civil Liberties in Australia.

26. CCL submits that a photograph on the front of a card is unnecessary. DHS and Department of Veterans Affairs (DVA) customer service staff will have readers and will be able to confirm that the photograph matches the cardholder themselves because the government has stated that it is planning to supply *uniform* readers to "doctors and others" and that this is part of the budget.[5]

27. If the photograph on the front of the card is simply for backup purposes, it will only have a limited utility; a photo would do little in helping someone prove they are entitled to concession benefits or other services as such features are only accessible by reading the chip (as opposed to concession cards today).

28. The KPMG report even acknowledges that the photo is just for the additional benefits of the card; use by emergency services personnel and as an all-purpose proof of identity card for example.

29. CCL is also concerned that the photo will unjustly discriminate against people with disabilities, and members of religious or indigenous communities for whom taking pictures (and being forced to publicly display them) represents a violation of their deeply held beliefs.

30. Moreover, there are members of the disabled community who might not want visible conditions so prominently displayed and recorded. With certain conditions, one's facial features may change over time more drastically than one's normally would. Members of the disabled community could thus be unfairly prevented from using their cards on account of inadequate facial recognition and thus subject to entrenched discrimination on account of their disability.

Because the card is not voluntary, there are no constraints on function creep, and a photograph appears on the front of the card; the 'Access Card' is a national identification card by stealth.

31. Simply stating that current proposal will not create a national ID card does not change the reality that in its current state the card has more than enough of the essential components for any national identification card scheme: it is mandatory,

[5] Budget Estimates, p. 78.

it will create a photograph identification database, and it has no legislative or administrative framework constraining the card's use and third party access.

32. While the government resents media and civil society that publicly label the current 'Access Card' a national ID card by stealth, it has done little to address its severest critics concerns. On the contrary, as discussed in more detail later in this submission, the government has consistently withheld information from the public and still refuses to commit to a legislative framework to constrain both function and access creep.

33. Using the United States experience with the Social Security Card as an example of function creep, CCL is concerned that the Australian database, from the outset, goes well beyond the Social Security Card system currently used in the United States. As the Taskforce pointed out in its initial discussion paper, what was once envisioned solely as a social security identifier has become a widely used number on everything from tax forms to bank accounts and credit cards. While the Social Security card is a good example of function creep, it pales in comparison to a card that is likely to be carried around in someone's wallet because of the frequency with which it must be or can be produced. Moreover, while the Social Security Card does, in fact, assign an identification number to all US citizens and residents, it does not reveal current addresses, birthdates, or dependents, and does not correspond to a photographic database. In the end, the United States has even better privacy legislation than Australia. Such legislation keeps the federal government in check by permitting citizens to sue if the government permits parties to see their records who are not specifically authorized to do under by the Privacy Act of 1974.[6]

The registration process and "POI confidence flag" system discriminate against various members of society and threaten to put more information than is necessary into the SCRS database.

34. Many people in Australia may be opposed to having their picture taken on religious or cultural grounds. Deeply religious and culturally sensitive Muslim women, for example, would be required to remove their hijab or burqa in violation of Islamic culture.

35. In addition to discrimination on account of a required photograph irregardless of one's disability, religion, belief, or practice, the KPMG report reveals that the registration process could lead to a an entrenched two tired identification scheme.

36. In order to maintain the integrity of card, the KPMG report proposes that those who cannot meet the minimum standards of registration should have a "low POI confidence flag" attached to the chip of the card. Presumably this would mean that those with a "low POI confidence flag" would have to produce further identification in order to claim their benefits. The system, from its inception,

[6] Privacy Act of 1974, 5 USC 552a.

would therefore entrench differing degrees of treatment; causing honest Australians who try to claim their benefits to feel like they are welfare fraud suspects.

37. CCL is concerned that disproportionately large numbers of the indigenous and immigrant communities will be associated with "low POI confidence flags" as members of both communities are more likely to be unable to produce the requisite documents on account of geography or social customs. Immigrants often arrive in Australia without many original documents and overseas documents cannot always be verified or are not always accepted.

38. While the Taskforce has identified this problem: "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."[7] None of the DHS Department of Access Card information mentions indigenous or immigrant communities that could be subject to this two-tiered card system.

39. Just as problematic and discriminatory is that the success rate of identifying people registered at mobile registration centers drops below 50%.[8] House-bound or elderly Australians in addition to those Australians in remote communities will thus disproportionately suffer from the government's desire to use photo-matching to verify identification.[9]

The new proposal is fraught with privacy concerns ranging from the possibility of private industry access to personal information to increasing threats from terrorists or computer hackers.

40. The government has yet to identify who will be able to ask to see the card, and who will be able to read the information contained on both the private and public sections of the chip. Currently without legislation prohibiting members of the private sector from demanding to see the card, the information on the card will be exposed to many thousands of more people than is necessary (for the operation of an improved benefits and concessions system).

41. Moreover, assurances that only "authorized people" will have access to information contained on the card provides little guidance as to who, in practice, will have access to exactly what information.[10] Such vague assurances also leave the decision to increase or decrease access to information contained on the chip and in the government's databases open to quick decisions by incoming and outgoing governments.

---

[7] Taskforce Discussion Paper.
[8] UK Passport Service, Biometrics Enrollment Trial, Management Summary.
[9] CCL notes, however, that according to the UK Passport Service, with respect to the population at large, biometric facial recognition was only successful 69% of the time, so the population. (UK Passport Service, Biometrics Enrollment Trial Trial, Management Summary).
[10] "Access Card at a Glance, 'What Information will the Access Card Hold?'" DHS Website.

42. Currently many private businesses offer discounts to citizens with various concession statuses. Will these businesses be able to obtain chip readers and what part of the information will they have access to? If businesses will be able to obtain readers, who is going to pay for their installation and monitor their use? As with any system, increased access leads to a greater chance of private information being disclosed.

43. Recent statements by Human Services Minister, Joe Hockey (the Minister) do nothing to assuage fears that businesses will be able to access at least some of the information on the card. In fact, during the past month, the Minister has lashed out not just at critics of the card, but also at banks and other industries. He cited them both for not voicing enough support for the card and not taking enough initiative to make their systems compatible with the new infrastructure being ushered in by the 'Access Card's' chip technology.[11]

44. The Minister has already indicated that he would not be immune to private-sector administration of some components of the card that could potentially put private information in the hands of businesses without consent from the Australian public. While Mr. Hockey insisted that the access card was not another Australia card and that there would be no "function creep" involving personal information, he stated "I would rather have a private-sector safety deposit box to hold that additional information in the case of a lost card.[12] CCL doubts whether the Australian public would be comfortable with private sector administration of such extensive personal information.

45. If the Minister is so comfortable with permitting the private sector to hold the personal information of the Australian public, CCL is concerned that the government would just as easily permit data farming and data-matching across the various databases (SCRS database and those kept by each participating agency). Data farming would permit businesses to use the system as a marketing tool to better sell their products to Australian consumers. Moreover, data-matching would allow business to target specific consumer who the data shows might be susceptible to buying their products. Again, the Australian public is unlikely to be comfortable yielding such vast amounts of information to business of all kinds looking to increase their sales and profit margins.

46. CCL is therefore concerned that the infrastructure necessary to support the introduction of the 'Access Card' will ultimately benefit private enterprises more than the public. On the one hand, private industry could simply be waiting to see if the smart chip technology is successful and thence to co-opt the technology once it has been determined that it is. On the other hand, the Minister has expressed his desire for private industry to actually install and operate their own

[11] "Hockey Hits Out At Smartcard Critics, Laggard Banks." *CIO: Australia's Magazine for Information Executives*, 24 July 2006.
[12] "Minister Flags Smartcard E-purse." *The Australian*, 4 July 2006.

readers which potentially could be used by consumers at the expense of the government. Private industries are unlikely to install readers and compatible technology without some financial incentive in hosting the transaction. Such transaction costs could foreseeably yield windfall payments to 'Access Card' operators at the expense of the Australian Government and its taxpayers.

Information on the public zone of the chip is potentially vulnerable to capture.

47. In addition to these questions, the government has yet to explain how the public and private zones of the chip are likely to work. Of concern is that information contained in the public zone is "potentially vulnerable to being captured electronically without the permission of cardholders."[13]

48. For instance, the government currently contemplates emergency services personnel being able to read the contents of the public section of the chip so what is to stop from every other person with a reader (whether they be a government employee, a public transport operator, or private parties) from seeing this information? Proposals such as requiring a pin number to access the information will only defeat the proposed benefit of having the information available in an emergency because in a serious emergency the victim is likely to be unconscious or in shock and thus preventing them from recalling the number.

49. Without enforced legislative restrictions on who can read the contents of the chip, any person with a chip reader could potentially capture information stored in the public zone.

The frequency with which the card will likely be used increases the chances that personal information could be compromised.

50. At the very least, the frequency with which the card will have to be used increases the likelihood that people will feel at ease carrying the card regularly and displaying it to more people than is absolutely necessary. The government is reinforcing this everyday utility by specifically marketing the card as an "all-purpose" high-quality identifier. The importance of the information displayed on the card (the unique and universal ID number) and the information potentially stored on the chip (medical information, contact information, and addresses) means, if anything, the government should be beginning with a campaign to reinforce the importance of keeping the card safe. The government's current approach will increase the chances of fraud resulting from information casually recorded from the card or from lost or stolen cards that were carried around when there was no need for doing so.

51. Briefly returning to a comparison between the proposed 'Access Card' and the Social Security Card in the United States, it is quickly apparent that unlike the

[13] Department of Human Services, *Health and Social Services Smart Card Initiative*, Volume 1: Business Case, KPMG, February 2006, *Public Extract* released June 2006. p. 19

Social Security Card, which is rarely carried and the number reluctantly divulged, one might be hard-pressed not find an Australian adult without their card in their wallet. In short, the likelihood that a unique identifying number or the information stored on the public space of the chip will be compromise is extremely high.

Increasing threat from computer hacking and terrorism.

52. CCL does not doubt that the government will take all available efforts to ensure that the security information contained in SCRS and the various databases maintained by government agencies and accessed through SCRS is not compromised by hackers, terrorist, or other criminals. However, given the highly-sensitive and concentrated information stored, and the number of highly-sensitive identification databases that have already been jeopardized around the world, no government could rule out the possibility that at some point information might be compromised. Storing vast amounts of information in one interconnected database enables a single security breach to have much larger implications than it otherwise might had the information been dispersed among the various agencies for whom such data is necessary.

53. For example, in the past few months the United States government admitted that the Social Security database of the Department of Veterans Affairs (DVA) had been compromised. The Agency learned, and was forced to publicize, that Social Security numbers of millions of veterans had been downloaded onto a hard-drive and removed from the DVA. While the computer has recently been found and the government believes that information had not yet been comprised, the DVA is still being forced to offer free credit checks to millions of Americans over the course of next year. While the breach was serious, it was at least contained within one specific agency. Cost in terms of finances and confidence associated with any breach of the proposed SCRS database could easily extend well beyond that experienced in the United States in this most recent incident.

CCL is also concerned that the proposed system may result in storing much more information than is needed or desired by consumers.

54. CCL is concerned by the contemplated scanning and storing of digital copies of documents used to initially verify a person's identity.

55. Foundation documents issued by the Australian government are currently not going to be stored by the new Data Verification System (DVS) being overseen by the Attorney General's Office. On the contrary, the DVS system, as CCL and other NGO's understand it, will provide real-time online verification of documents issue by the Australian government (Yes/No answers with no digital copies stored).

56. CCL is concerned that either the DHS and the Taskforce might not have understood the new DVS proposal, or worse, might be ignoring it in favour of an

alternative registration system that would involve actually scanning and storing Australian government-issued documents.

57. Under both the DVS and the DHS proposal for the 'Access Card' the government seems willing to scan and store foundation documents not issued by the Australian government. Doing so vastly increases the amount of information potentially open to capture by unauthorized parties. Many of these foundations documents contain information that is simply not necessary for the operation of the new card or for initial and subsequent verification purposes. This scan, store, and verify later approach will result in anther form of discrimination against people born overseas because they will be exposed to more serious breaches of their privacy.

The additional benefits of the card raise their own set of security concerns which have yet to be identified or addressed by the government.

58. The government is largely relying on the additional benefits of the card to distract Australians from the fact that they will be branded with a unique identification number corresponding to a new intrusive photograph and information database. However, these additional benefits themselves are of concern as they increase both the amount of information open to capture, and the potential that such information could be captured by unauthorized parties.

59. CCL has already noted how and why access by unauthorized parties to volunteered personal information contained on the card and on the chip is a concern. However, CCL is also concerned by the government's commitment to making private information easily available to members of the public. While maintaining an accurate database should be a priority, and encouraging open and honest record-keeping reinforces open and honest governance, an individual's ability to access and update information stored on the card through an online password/login could threaten the integrity of the system. Computer hackers are already quite experienced with capturing passwords and usernames from recently used computers and could quite easily retrieve and/or change information that is deeply personal and potentially life-threatening during an emergency.

60. In addition to greater chances of theft, the government has not identified whether it intends to limit the amount and content of information stored on the chip. While the government continues to assure the public that information on the chip will not be accessed by "unauthorized persons," the reality is that many consumers could be lulled into putting more private information onto the card than is actually useful. Individuals could be inadvertently subjecting themselves to greater violations of their privacy on account of a database, which like all databases, can never be 100% secure.

61. Moreover, CCL has questions concerning how often the government intends to enable consumers to update their information to ensure it is accurate. Additionally, will doctors be able to verify the health information that consumers

place on their cards? Inaccurate or outdated medical information could be potentially life-threatening should emergency services personnel rely on the information during an emergency.

62. Indeed, one of the most often-touted benefits of the "Access Card" is that emergency services personnel will be able to use the information on the card to treat their patients. As mentioned above, either information must be easily accessible to such personnel without a pin number, or this additional benefit will do little in an emergency situation where one is unconscious or in shock.

63. Further questions arise surround this purported benefit. First, emergency services personnel trained to respond and treat symptoms of medical conditions may continue to treat patients without looking at the card in the first place. A person might not be carrying the card during an emergency, and quite often one could waste precious minutes looking for the card instead of preventing further harm. Second, will first-responders come to rely solely on the card instead of asking or confirming with their patients whether they have any medical conditions before deciding on a course of treatment? Giving someone the wrong blood-type, for example, is often fatal, and relying solely on the information on the card could quite easily lead to such an occurrence.

64. Finally, the government has cited the ability to populate forms as a means to save consumer's time when dealing with government agencies. However, as media reports have pointed out, convenience can often lead to greater opportunities for identity theft. Thieves already intercept electronic and regular mail and use the information contained therein to open new accounts or access funds from existing ones.[14]

Increased access by law enforcement agencies to more personal information continues to be a motivating factor behind the 'Access Card.'

65. The government has stated that it does not intend to re-examine or re-structure the various law enforcement agencies' ability to access information held by different government agencies: "Nothing will change in terms of the powers of those people."[15] This is of particular concern in light of the fact that Australia has never before had a photographic database containing the picture of virtually every Australian or comprehensive system whereby Australians' actions can be tracked like never before.

66. Additionally, the government has not ruled out using biometric photographs stored in the SCRS to match photographs taken by CCTV cameras of suspected subjects. (Budget Estimates, p. 85) CCL is concerned because photo-matching often leads to false-positives and therefore false accusations levelled against innocent people. Unlike fingerprints, the American Civil Liberties Union notes

[14] "Vigilant Teller Unmasks Major Identity Theft Ring." *Sydney Morning Herald*, 12 July 2006.
[15] Budget Estimates, p. 75

that peoples' faces do not stay the same over time, "these systems are easily tripped up by changes in hairstyle, facial hair, or body weight, by simple disguises, and by the effects of aging."[16]

67. The ACLU has also highlighted that, "questions have been raised about how well the software works on dark-skinned people, whose features may not appear clearly on lenses optimized for light-skinned people."[17] This is of particular concern because false-positives might occur with much greater frequency among darker-skinned people and thus potentially lead to a greater number of false accusations being made against immigrant and indigenous communities here in Australia.

68. ASIO has also stated that it was not consulted in the Privacy Impact Assessment, though the government did consult ASIO about the potential benefits and uses of earlier versions of the 'Access Card,' indicating a desire for the card to benefit security agencies in addition to consumers. In addition to exemplifying a form of function creep, CCL submits that the technology might ultimately not benefit security agencies. A study using facial recognition technology in Tampa, Florida, for instance, failed to recognize a single suspect while managing to generate a number of false positives.[18]

69. Ultimately, CCL believes that the motivations behind the 'Access Card' are suspect in light of the timing of the recent decision to review the need for a national identification card in the wake of Sept. 11th attacks and the bombings in Bali, Madrid and London. Only after determining that Australians were still firmly opposed to the introduction of an identity card did the government reveal its plan for a smartcard that would assign a unique identifying number to virtually every person in Australia. If the government sees the new 'Access Card' as way to make Australians more secure it should not make the case for the card based on overstated claims about the level of welfare fraud or promises of convenience for consumers.

In addition to the numerous uncertainties surrounding the current proposal, the government's decision not to release the Privacy Impact Assessment and to censor several portions of the KPMG report is contrary to open and honest governance. Such actions will continue to undermine the public's trust throughout the proposed consultation and implementation process.

70. CCL is concerned that the Privacy Impact Assessment commissioned by the government from Clayton Utz has still not been released despite calls from several members of Parliament and numerous NGO's. The government has given various reasons for its decision to withhold the PIA ranging from its redundancy to it being Cabinet-in-confidence. If the report is truly redundant, the government

[16] "Q & A on Facial Recognition." *American Civil Liberties Union*, 2 September 1999.
[17] "Q & A on Facial Recognition." *American Civil Liberties Union*, 2 September 1999.
[18] "Q & A on Facial Recognition." *American Civil Liberties Union*, 2 September 1999.

should not fear its release, and if the card is truly aimed at consumer benefits and not security, there should be little harm in releasing to the public.

71. While the government released the KPMG Business Case, which was very supportive of the government's initiative, its release was heavily censored. The censored materials inhibit the ability of the public to determine whether the proposal is worth the serious risks to personal privacy and civil liberties. Such actions further undermine public trust in the government and its motivations.

72. CCL is also concerned that the Minister has heeded neither the recommendations of the KPMG report nor those from his own DHS smartcard taskforce regarding setting up independent and well rounded bodies to research and oversee the implementation of the new proposal. The KPMG report recommended that the Privacy Commissioner sit on an independent board specifically constructed to implement the proposal, while the DHS report advocated that the Office of the Access Card be located outside of the Minister's DHS.

73. Finally, the government has admitted that there was "no broad-ranging consultation" with privacy or consumer groups in the development of the business case despite what the KPMG report explicitly states.[19] The lack of any community input in the early stages of the proposal is upsetting considering the scope and impact of the project.

Other Considerations

74. Evidence from various nongovernmental organizations and advocacy groups suggests that the government's proposal is likely to cost much more than the current proposal ($1.09 billion from 2006-2010). First, the much-touted additional benefits of the new 'Access Card' such as emergency medical information or the card's ability to deliver disaster relief have not been factored into the government's calculations. Second, and more importantly, all government projects of this scope inevitably encounter unforseen technological or implementation problems. There is little reason to think that a project of this magnitude will prove to be the exception.

75. CCL is also concerned that the 'Access Card' has the potential to be used as a means to further restrict the use of government entitlements. The card could prevent recipients purchasing alcohol, personal items, or any other product not deemed essential or beneficial.

76. CCL, like many other groups representing public constituencies, worries that the access card may be a way to subsidize the introduction of new technology ultimately more suited to implementation and use by the private sector. Thus far the banking industry has yet to consider the move to "smart chip" technology

[19] Budget Estimates, p. 94

necessary. Will private industries that wish to benefit from the widespread use of the new technology reimburse the government for its implementation?

77. Finally, CCL would like to ask the government, in the spirit of open and honest discussion, to explain to the public from where the funds for this proposal will come. CCL believes that in addition to the human rights and privacy implications of the project, the budgetary issues should be openly debated in the coming months so that those constituencies that might be affected by changes in the budget are aware of all of the project's implications.

CCL proposals for constraining infringements against civil liberties and personal privacy; suggestions on how to improve this dangerous legislation.

78. **Ultimately, CCL believes that despite whatever constraints are put in place to prevent function creep and the theft of a variety of personal information, there are alternatives to the 'Access Card' that would not create a citizen data/photo base so closely resembling a National ID Card.** Medicare cards could be upgraded to utilize smart chip technology without assigning unique, system-wide identification numbers to virtually every Australian. The creation of vast photograph and information databases that are potentially subject to security breaches or abuse by unauthorized personnel goes well beyond the need to simply upgrade the system by which benefits are distributed.

79. MAKE THE NEW CARD OPTIONAL for those who are willing to sacrifice privacy for whatever convenience they see the card will bring.

80. DROP THE PHOTO ON THE FRONT OF THE CARD or at the very least make the photograph on the front of the card optional. The current proposal may force people to violate their deeply held religious or cultural beliefs or discriminate on the basis of one's disability. Moreover, CCL submits that such a photo is not necessary if all members of the government who need to use the card will have access to the same chip-reading device.

81. LEGISLATION SPECIFICALLY PROHIBITING AND PREVENTING FUNCTION CREEP WITHOUT PUBLIC DEBATE AND FURTHER LEGISLATION. Such legislation should specifically mandate that new uses of card must go through a process of public consultation and debate followed by legislative approval before being instituted. This legislation would reassure the public that the new card will not become a new national identification scheme. The Legislation should guarantee public hearings, submissions, and legislative and administrative debate. CCL notes, however, that such legislation is only as good as the initial authorizing 'Access Card' legislation. If the initial authorizing legislation does nothing to limit public and private use of and access to the new card (and corresponding databases) then legislation preventing further function creep loses much of its relevance.

82. LEGISLATION PROHBITING PRIVATE PARTIES FROM DEMANDING TO SEE THE CARD. Aside from government officials tasked with the distribution of benefits or concessions, private parties should be required to accept another form of identification. Without this piece of legislation the 'Access Card' truly is mandatory because the private sector is likely to look to the card as a new superior form of identification. In fact, the government has been encouraging big business to display more public commitment to using the new technology, reinforcing its critics' worst fears that whether or not someone needs to have a card, they will be forced to get one to meet everyday demands for identification in the private sector.

83. LEGISLATION PROHBITNG THE PRIVATE SECTOR FORM ACCESSING THE SCRS DATABASE OR CORRESPONDING DATABASE'S IN THE DHS UMBRELLA. Legislation should prevent public information from being "sold or borrowed" to private enterprises for any sort of commercial purposes. This concept is often known as data-farming. Moreover, legislation should prevent the government from tracking individual use of the card across the range of government services for public or private use. Most Australians would feel their privacy had been violated if the government embarked on any sort of data-tracking scheme.

84. TIGHTEN EXISTING PRIVACY LEGISLATION. The Privacy Act was created in the wake of the defunct Australia Card. It was, therefore, not designed to manage a comprehensive national database like the one that will issued in by the 'Access Card.' The government should at least acknowledge that the creation of this new comprehensive information and photograph database, to many, closely resembles an national identification scheme. Recognizing this legitimate concern, rather than attacking critics, the government should reassure the public by honestly examining how the new proposal will work with existing privacy legislation by holding public hearings and accepting submissions from concerned citizens and advocacy groups. If the public then sees a need to re-examine existing privacy legislation, options should be explored before the 'Access Card' is implemented.

85. CONDUCT A PUBLIC REVIEW OF LAW ENFORCEMENT'S ABILITY TO ACCESS INFORMATION FROM THE SYSTEM. This review should include access by ASIO, AFP and local police and should pay particular attention to the use of CCTV photo-matching. As discussed above, public hearings and invitations for submissions from concerned members of the public or advocacy organisations should be welcomed to reassure Australians that the new system will not become something the government promised it would not (a new national identification scheme).

Conclusion

86. Despite our willingness to discuss solutions to the highly problematic 'Access Card' proposal as it now stands, CCL will not support any proposal resembling a national identification scheme. This is particularly true when the government has refused to answer many questions and to release the Privacy Impact Assessment commissioned with the KPMG Business Case. CCL will continue to monitor threats to civil liberties such as the potential for discrimination, public and private sector abuses of personal information, and the ways in which law enforcement will access and utilize the newly stored information.

87. CCL would be happy to elaborate further on any of the above points or produce further submissions once the government releases more information about the current proposal.

Yours faithfully,

Stephen Blanks
Secretary, NSW Council for Civil Liberties