Australian Government

Office of the Privacy Commissioner

Inquiry into the *Human Services (Enhanced Service Delivery) Bill 2007*

Submission to the Senate Finance and Public Administration Committee

February 2007

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner ('the Office') is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the *Privacy Act 1988 (Cth)* ('the Privacy Act'), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations.

Background

2. The Office welcomes the opportunity to make this submission to the Senate Finance and Public Administration Committee's Inquiry[1] into the Human Services (Enhanced Service Delivery) Bill 2007 ('the Bill').
3. The Office made a submission in January to the Office of Access Card on the exposure draft of the Bill[2]. As well, in August 2006 the Office made a submission on the Discussion Paper issued by the Department of Human Services Access Card Consumer and Privacy Taskforce[3].
4. The Office considers that the development of dedicated legislation on the access card and accompanying system presents an opportunity to prescribe the purpose, functions and practical operation of the access card system in a way that may benefit all Australians by safeguarding their personal information and respecting their privacy. In its submission to the Office of Access Card's Consumer and Privacy Taskforce, chaired by Professor Allan Fels AO ('the Fels Taskforce'), the Office highlighted the role of such legislative protections as a necessary element of a robust privacy framework for this important initiative.
5. In the Office's view, it is important that the legislation includes the types of protections and accompanying oversight mechanisms that the community is likely to expect.

[1] Details of the Inquiry are at http://www.aph.gov.au/Senate/committee/fapa_ctte/access_card/index.htm

[2] The Office's submission to the Office of Access Card on the exposure draft of the Human Services (Enhanced Service Delivery) Bill 2007 is available at http://www.privacy.gov.au/publications/accesscardexposuresub.html

[3] The Office's submission to the Consumer and Privacy Taskforce is available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html

General comments

6. In noting the timeframe established for the implementation of the access card system, the Office believes it is important that legislative measures do not pre-empt the finalisation of important design and policy considerations. In the Office's view, decisions on those considerations should be open to public scrutiny and settled, before enabling legislation is enacted. If not, there is a risk that privacy enhancing design and policy options could be prematurely excluded, to the overall detriment of the initiative and community support of the system.
7. In particular, the Office notes the importance of ensuring that the Bill does not establish a legislative framework, whether intentionally or otherwise, that relies on or assumes the existence of a unique personal identifier (UPI) for each card holder, such as a number, that is then held and shared by various agencies or organisations. This risk is referenced in the Office's comments regarding the requirement to include a participating agency 'flag' on the register (s 17, item 14 – discussed below at paragraph 20(f)).
8. The risks of such a system are discussed in detail in the Office's submission to the Fels Taskforce[4], but include:
   - significantly expanding the capacity for datamatching between agencies or organisations in ways that may go beyond public expectations;
   - creating pressures to allow uses of personal information in ways not currently envisaged by the legislation; and
   - increasing the risk of interferences with privacy by creating an infrastructure that could allow the linking of data from currently disparate data sources, possibly including in the private sector.
9. The Office encourages further consultation with relevant privacy and technology experts to explore design options that avoid such risks. Legislation can then be pursued to give effect to such agreed designs.

Detailed comments on the Bill

10. For ease of reference, these comments will generally be grouped under the sections of the Bill.

Part 1 – Introduction

11. The Office welcomes the enumeration of the objects and purposes of the Bill. The Office notes section 6(2), which states that "it is also an object of this Act that access cards are not to be used as, and do not become, national identity cards". The Office previously commented that the original wording of this object, which stated that it was "not an object of the Act that access cards be used as national identity cards", should preferably prohibit

[4] See paragraphs 185-189, 204-207 and 211 of the Office's submission, available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html.

the access card being used as a national identity card. The Office welcomes this change.

12. It may further clarify the policy intent if the objects clause expressly included reference to the access card number, and provided that it is not to become a unique identifier for each individual, which could be used, shared or adopted by Australian Government agencies, State and Territory agencies, or the private sector.[5] Such a protection would be consistent with the policy intent of National Privacy Principle 7 (on unique identifiers) and the protections afforded to individual's tax file numbers.[6]

13. The Office welcomes the requirement for any administrative policy statement that may be prepared by the Minister pursuant to s 8 being tabled in Parliament.

14. However, the content that may be included in such a statement is unclear to the Office, as is its precise function and relationship to the Bill's objects and purposes. It is assumed that such statements will assist in defining the manner and scope in which discretion is exercisable by the Secretary and delegates in a range of provisions under the Bill. If so, it may be useful to redraft the provision to make this intention more apparent.

Part 2 – Registration

15. Section 13(1) states that "You, or someone else on your behalf, may apply…" for registration.[7] The Office suggests further clarity regarding how this "someone else" is determined and what authority they must have to apply on an individual's behalf (for example, status as a parent, guardian, carer or legal representative, or the Department of Human Services ('the Department'); and whether written authority alone would be accepted). A clearer expression of policy intent or definition in the legislation could be useful to avoid multiple, unwanted or fraudulent applications.

Information on the register

16. The development of the access card system would be the first time an Australian Government database has held a digitised signature and biometric photograph of the majority of the adult population. The Office has previously noted its concerns about the collection of these items.[8] The Office is pleased that the Fels Taskforce report reflected the Office's recommendation that rigorous controls on unauthorised access and improper disclosure be put in place to safeguard these items wherever held, including on the register, chip and card surface.[9]

17. An effective way of minimising interferences with privacy is to only collect personal information where there is a specific, lawful and necessary

[5] National Privacy Principle 7 prevents many private sector entities from adopting Commonwealth identifiers, but does not cover all businesses or individuals.
[6] Also see the see the discussion at paragraphs 64-68 in relation to unique identifiers
[7] See also sections 14, 23 and 24.
[8] See paragraphs 67 and 117-137 of the Office's submission to the Fels Taskforce, available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html.
[9] See Fels Taskforce Report No. 1, Recommendations 16 and 17.

purpose for doing so. This is an underlying principle of privacy law and practice. The Office welcomes the decision not to collect information for inclusion on the register regarding an individual's place of birth.

18. In some cases it remains unclear to the Office whether it is necessary for particular types of personal information to be collected and stored on the register (s 17). The Office submits that the register may not need to include personal information that is required to specifically determine an individual's eligibility for entitlements. Such personal information would best be collected by the administering agency for that entitlement, rather than into a central database.

19. The Office submits that the guiding policy setting for the register should be to collect the minimum amount of personal information, and that this should be reflected in the legislation.

20. In regard to specific types of information currently prescribed in the Bill, the Office makes the following comments:

    a. *Citizenship/residency status (item 3):* Given that the access card is not a citizenship document, it is unclear why residency status need be stored. If certain benefits accrue depending on residency status, the Office suggests that the relevant agencies collect this information independently of the register, or the card could be appropriately limited in its functionality without retaining that information on the register.

    b. *Indigenous status (item 4):* The Office notes that this item has been added since the exposure draft was released. It is not clear why an individual's indigenous status is information which is necessary to be collected or retained on the register. If certain benefits accrue depending on this information, the Office suggests that the relevant agencies collect this information independently of the register.

    c. *Sex (item 5):*[10] The Office suggests that further consideration be given as to whether an individual's sex is necessary to be stored on the register, as distinct from being information necessary for particular agencies to provide certain services. The Office previously raised this issue in relation to the former terminology "gender" in our comments on the Exposure Draft of this Bill. The Office remains concerned about how the preferences of transgender persons will be respected when collecting this information, particularly given the sensitivities that are likely to arise and the implications for accuracy of personal information. It is unclear that a change in terminology addresses this challenge. Further consultation with transgender groups may be of benefit before law is enacted.

    d. *Contact details (item 6):* The Office does not consider that an individual's residential address is necessary as a mandatory inclusion on the register. There may be valid reasons why an individual would prefer that their residential address is not recorded in this register (as, for example, in a domestic violence situation).[11] Noting the first two

[10] See also s 34, item 3 (information on card chip).
[11] The Bill's special provision for individuals under witness protection (s 80) reflects this notion.

objects of the legislation,[12] the Office submits that individuals should be able to elect whether one or both address types are stored on the register.

e. *Signature (item 9(g)):*[13] The Office has previously questioned the need to include a digitised signature on each of the register, card chip and card surface, given that it would appear to have limited value to government and consumers, and the potential risks of its use in identity fraud if any of those systems are inappropriately accessed.[14]

f. *Participating agency flag (item 14):* The Office is unsure of the design implications of this item.

The storage of a 'flag', rather than an agency specific identifier, may have unintended consequences. It may suggest that each agency would need to retain a common identifier to enable them, in approved and appropriate circumstances, to exchange information for the delivery of programs (see also paragraphs 7-8 above). However, the creation of such an infrastructure also leaves open the possibility of future data sharing that may go beyond individuals' expectations. The Office discussed the risks of such designs in its submission to the Fels Taskforce.[15]

The Office would encourage further consultation with relevant privacy and technical experts to avoid a system which allows the linkage of identifiers between agencies.

g. *Death (item 16):* Noting the discussion at paragraph 18 above, the Office understands that it may be necessary for this information to be passed on to agencies, but it remains unclear why this information would need to be retained on the register. The issue of retention of information is discussed below at paragraphs 26-27.

h. *Benefit card information, copies of proof of identity documents, and other information necessary for administration (items 7, 12 and 17):*[16] Information recorded under these items is determined at the discretion of the Secretary. To avoid greater collection of information than is necessary, it would be desirable to ensure that these provisions are not too open-ended. The provisions may also limit the effectiveness of s 20, which precludes additional information being stored on the register.

21. Item 17(a) of s 17 provides for the inclusion on the register technical or administrative information which does not expressly identify a person by name or identifier. The Explanatory Memorandum describes this as including audit logs or chip serial numbers, where they are reasonably

[12] Section 6(1)(a) and (b) – These refer to reducing complexity for those "most in need of assistance", and facilitating "user-friendly" access.
[13] See also s 34, item 6 (information on card chip).
[14] See paragraph 67 of the Office's submission to the Fels Taskforce, available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html#mozTocId807918.
[15] See paragraphs 185-189, 204-207 and 211 of the Office's submission, available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html.
[16] See also s 34, item 10 and 17 (information on card chip).

necessary for the administration of the Register or an access card. While the Office notes this limitation on the information which may be recorded in the register, it also notes that personal information may identify an individual in ways other than by name or identifier. It appears that this requirement will prevent the recording of identifiers issued by other government agencies, including participating agencies. It is unclear what other effect this limitation may have on the Secretary's ability to determine additional information to be recorded on the register.

22. Item 17(b) of s 17 provides for other information to be stored on the register, as determined by the Minister (by legislative instrument), for the purposes of the Act. The Office welcomes this opportunity for parliamentary scrutiny (by way of disallowable instruments), and the link provided to the Act's purposes. The Office also notes that this power may be delegated to the Secretary (s 68(1)(b)), and this is discussed further at paragraph 72.

23. The number and nature of types of personal information that may be stored on the register is a key privacy issue. As noted earlier, good privacy practice is promoted by ensuring that only necessary information is collected.

24. Accordingly, the Office suggests that a general provision could be provided, to the effect that any powers to make decisions to expand the permitted contents of the register should be done in consultation with the Privacy Commissioner. A possible model of such a mechanism is available in section 85ZZ(1)(b) of the *Crimes Act 1914* concerning the Commonwealth spent convictions scheme. Under this provision, the Privacy Commissioner is required to advise the Minister for Justice and Customs on possible exclusions to the scheme.

25. The Office suggests that the provision to scan and retain copies of proof of identity documents (s 17, item 12) raises privacy issues and should be modified, if not removed. Such documents may include much personal information that is not necessary for the access card system, including about third parties. The Fels Taskforce also recommended against the scanning, copying or keeping on file of proof of identity documents once verified.[17]

26. The Office notes that the Bill is silent on the period for which scanned documents will be stored on the register. While the Office's preference is that this form of collection not occur, some privacy protection may be afforded by a provision that limits the retention period, including by providing that documents not be retained once verified.

27. The Bill does not prescribe procedures for the deletion of information from the register more generally, once it is no longer necessary to retain it (for example, when an individual dies or voluntarily de-registers). The Office notes that unnecessary retention of information can have privacy implications. While these matters may be contemplated for the second

[17] See Consumer and Privacy Taskforce on the Health and Social Services Access Card, Report No. 1, September 2006 ('Fels Taskforce Report No. 1'), Recommendation 20 and discussion at pp 45-9, available at http://www.accesscard.gov.au/various/Consumer_privacy_rp2.pdf.

tranche of legislation, the Office submits they should not be left to existing legislation such as the Privacy Act, which may not, in some circumstances, provide suitable protection (such as for deceased persons' information).

28. The Office remains of the view that there are important distinctions between information which needs to remain on the register, information which need only be stored temporarily,[18] and that which need not be stored at all.

29. Some individuals may prefer to retain more direct control over their personal information including, where practicable, by storing it on the chip alone. Where the intention for 'duplicated storage' is for greater individual convenience (such as minimal re-registration if a card is lost), the legislation could allow for such storage at the individual's discretion.

Discretionary functions of the Secretary and delegates – generally

30. The Office recognises that it is common and appropriate for legislation to provide mechanisms to delegate powers. Such provisions will often relate to routine or administrative matters.

31. The legislative protections accompanying the introduction of the access card are an essential element in promoting community confidence. The access card system is unique in character, in that it will cover the majority of the Australian adult population, facilitating the collection, retention and handling of personal information on a significant scale. Accordingly, even those matters that may ordinarily be considered routine or administrative are likely to have consequences for how personal information is handled.

32. Consequently, the Office suggests that the Bill should reflect a general policy of ensuring that decisions which affect personal information are subject to appropriate oversight, including where such decisions go to administrative matters.

33. There are a number of areas of the Bill which the Office believes should be subject to additional oversight mechanisms, independent review, clear Ministerial direction or specific criteria, including determining:

    a) what proof of identity (POI) information and documents are needed for registration (s 13(2));[19]

    b) the form or manner in which the register may be kept;[20]

    c) what information about an individual's benefit cards will be held on the register and the chip (respectively – s 17, item 7; and s 34, item 10);[21]

    d) what proof of identity documents (or information about those documents) will need to be scanned and placed on the register (s 17,

[18] Section 19 refers to the temporary holding of information, but only for the purposes of transferring to the chip. Notably, it does not indicate the length of time that qualifies as temporary.

[19] These determinations (apart from under s 13(2)(b)(ii)) would be subject to any identity guidelines issued under s 66.

[20] Section 16(3) notes that register is not a legislative instrument.

[21] Sections 17(2) and 34(2), respectively, state that neither determination is a legislative instrument.

item 12);[22] and

e) when applying for an access card, what "other specified information" or documents that the Secretary deems necessary: (i) to be satisfied of the applicant's identity, or (ii) to obtain information required for the card or the register (s 23(2)(b)).[23]

34. In particular, the Office suggests that items a), d) and e) above should be subject to parliamentary scrutiny. The absence of such scrutiny could reduce the benefits of prescribing, in statute, the types of personal information that may be collected for the purposes of the access card.

35. In addition, the Office repeats its suggestion (see paragraph 24 above) that the Bill could usefully promote community confidence by including a general provision that these powers be exercised in consultation with the Privacy Commissioner. Section 212(2)(a)(vi) of the recently enacted *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* provides a possible example of such a provision.

Part 3 – The Access Card

36. The Office has noted above (see paragraphs 16-29), in regard to collection for the register, the importance of ensuring that personal information is only collected where necessary.

37. Similarly, the Office notes its earlier comments cautioning against unnecessarily duplicating collection and storage of personal information on the chip, card and register (paragraph 29) and the need for additional oversight where discretionary powers affect the handling of personal information (paragraphs 30-35).

Form of the access card

38. More specifically to this Part, the Office notes that the form of the access card is determined by the Minister (s 27(4) and (5)). This decision would be particularly important if (drawing on clause 27 of the Explanatory Memorandum) the card were adapted in the future in response to emerging technologies. It is often the case that new technologies raise new privacy issues.

39. The Office submits that the determination of this issue could be strengthened by subjecting it to parliamentary scrutiny (for example, as a disallowable instrument), independent review and/or public comment. Doing so could also increase public confidence, transparency and accountability. This would be consistent with other powers in the Bill that are subject to legislative oversight.

40. The Office also notes that a general provision, as suggested above at paragraphs 24 and 35, requiring consultation with the Privacy Commissioner on the operation of the Act may be appropriate.

[22] Sections 17(2) states this is not a legislative instrument
[23] Any s 66 identity guidelines must be "taken into account" under 23(2)(b)(i), but not 2(b)(ii).

Information on the surface of the access card

41. The Office welcomes the choice to display an individual's preferred name on the card upon request, and that displaying one's date of birth is optional (s 30, items 1 and 6). It is important that these options and other such 'requests' are well explained, publicised and easily exercisable.

42. Notwithstanding the Office's concerns over certain items on the surface of the card (as previously raised in the Office's submission to the Fels Taskforce, and by the Taskforce itself[24]), the Office welcomes the limitation of information held on the card's surface under section 30 (and for the card chip at s 34).

Information on the card chip

43. The Office reiterates the need to ensure robust protections against unauthorised access and improper disclosure of information held on the card chip, and elsewhere in the access card system.

44. The Office understands that the content in the individual's area of the chip will be limited by the physical capacity of the chip and any legal constraints, including any regulation that is introduced in subsequent legislation.[25] The Office welcomes proposals to maximise consumer choice in this matter. Nevertheless, in the interests of data integrity and security, consideration should be given (possibly in future legislation) to dealing with the risk of viruses, 'spyware' and other inappropriate software being stored on the chip, with the intent of modifying any person's card or interfering with the access card system.

45. Item 4 of s 34 states that a residential address must be stored on the chip. While noting this is a lesser requirement than for the register (s 17, item 6), the Office believes that the individual should be able to choose whether residential *or* postal address is stored on the card chip.

46. Item 14 of s 34 requires information relating to the registration status of the individual be stored on the chip. This will indicate whether the proof of identity has been assessed as "full" or "interim" status. It is unclear why this information is necessary on the chip, which may be able to be read by participating agencies, concession providers or readers held by other bodies. The risk that this information could establish two classes of recipients of goods or services, even if this involves a tacit rather than explicit differentiation by providers, could be mitigated by storing this information, if it is necessary to be stored at all, only on the register, as provided by s 17 at item 8.

[24] See, for example, paragraphs 118-122 of the Office's submission, available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html. See also Fels Taskforce Report No. 1, Recommendation 15.

[25] See Explanatory Memorandum, clause 33.

Ownership and use of the access card

47. The Office understands that the intention of s 41 is to regulate use of the card by all officers of participating agencies. However, given the broad terms of the statutory purpose, the Office queries whether the provision would unintentionally permit use of the card by such an officer who would not otherwise be able to use the card at all (provided they do so for the purposes of the Act).

48. The Office submits that more robust protections may be afforded by inserting a provision, under Part 3 Division 6, *proscribing any use* of the access card by Commonwealth officers (other than "authorised persons" in participating agencies) unless the individual chooses to allow it.

Consenting to allow agencies to use an access card beyond the purposes of the Act

49. If an individual may consent to the use of their access card outside of the purposes of the Bill (s 41(b)), it is important that the consent be fully informed and voluntary. This provision could refer to s 62 (abuse of public office) to discourage improper seeking of consent.

50. In addition, the Office suggests that "express" could be inserted before the word "consent" in section 41(b). This may ensure that a clear and unambiguous statement of consent is required from an individual that they agree to their access card being used by a Commonwealth officer in a participating agency for purposes outside the Act.[26]

No requirement to carry an access card

51. The Office welcomes the intent of s 42, which states "you are not required to carry your access card at all times". However, the qualification "at all times" could leave open the prospect that individuals may, in future, be required to carry an access card when in certain places or carrying on certain activities. This would seem to create a tension with the stated policy intent that individuals need only present an access card when they choose to seek benefits and entitlements related to health and social services. The Office suggests that an alternative drafting of this section might state: "There is no requirement to carry your access card".

Part 4 – Offences

52. Generally, the Office notes that Part 4 tends to focus on offences relating to access cards rather than the register. For example, the offences do not appear to deal with unauthorised access to or interference with the register, either by Commonwealth officers or others. The Office believes such matters should be addressed in future legislation.

[26] The Office's Guidelines on the National Privacy Principles explain that "Express consent is given explicitly, either orally or in writing." In the Office view, express consent provides that an individual make an active decision as to how their personal information may be handled. In contrast, implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation.

53. While the Office supports the inclusion of criminal offences in regard to the access card, individual offences under the Bill may be difficult to prosecute and prove (such as showing 'intent', particularly under the criminal standard of 'beyond reasonable doubt'). This may reduce the deterrent effect and the likelihood that an aggrieved individual would obtain satisfaction.

54. It is important that penalties and offences (such as those relating to 'requiring production') are clearly articulated, effective and enforceable. The Office notes that criminal offences will generally require intent to be proven. The Office notes, for example, that while ss 45-46 do not refer to "intentionally requiring" the production of the Access Card, the Explanatory Memorandum refers to s 5.6 of the Criminal Code, which requires that the person commit the proscribed conduct intentionally. Accordingly, it may be useful to include civil offences alongside criminal ones, as is found in other legislation.[27]

55. Civil penalty provisions may provide individuals with an alternative means of redress, and minimise the unchecked misuse of access cards due to a lack of evidence or resources to pursue criminal charges.

56. The arrangements for the handling of tax file numbers may provide another useful model, whereby an individual may seek remedy under the regulatory mechanism of the Privacy Commissioner's Tax File Number Guidelines, issued under s 17 of the Privacy Act 1988. At the same time, criminal action may be pursued against an individual who, in the handling of tax file numbers, commits offences against the *Taxation Administration Act 1953 (Cth)*.[28]

57. Review of the effectiveness of the offence provisions after a certain period may also assist in protecting individuals and minimising unconscionable conduct.

Division 2 – Offences for requiring production

58. The Office welcomes efforts to protect individuals from improper demands for production and refusal of services, including where such demands are oral, in writing or in another way and meet a test that the individual would "reasonably understand" that they are being required to produce an access card (ss 45-46).

Division 3 – Offences for doing things to access cards

59. The Office is uncertain whether s 47 intends to encompass damage that occurs unintentionally. The Explanatory Memorandum refers to intentional damage, but the clause itself does not. The Office also notes that it may be questionable whether it would always be practicable to show 'intent' for such offences.

[27] See, for example, Chapter 9 of the *Corporations Act 2001* (Cth), Part 9.4B.

[28] Specifically, s.8WA places restrictions on unauthorised requirements or requests that a tax file number be quoted. S.8WB places restrictions on the unauthorised recording, maintaining a record of, use or disclosure of a tax file number.

60. The Bill does not appear to provide an offence for *possessing* someone else's card without consent, or for *copying* information from a person's access card (including from the chip), or from the register, without authorisation. Section 57 proscribes the copying or recording of the access card number, photograph or signature on the surface of an Access Card, however this does not appear to address the potential that a person could copy information from the chip, or from the register.

61. The Office questions whether "damage" under s 50 would include 'modifying' one's card, particularly by using the individual's area to install software, to dishonestly obtain an advantage. The Office also notes that this provision is unlikely to apply where the intent is merely to interfere with the system, and submits that the latter should also be considered under the offence provisions.

Divisions 4, 5 and 6 – Other offences

62. The Office welcomes the offences relating to unauthorised recording and use of the access card number (s 57). These offences would be reinforced if specific secrecy provisions were enacted to protect the information held on access cards, chips and the register.

63. In Division 5, ss 58 and 59 make it an offence to make a false or misleading statement, or provide false or misleading information in relation to an application for registration or access card. The Explanatory Memorandum indicates that ss 58 and 59 only intend to proscribe *deliberately* false or misleading statements, and makes reference to s 5.6 of the Criminal Code which requires that the person commit the proscribed conduct intentionally. However the Office queries whether this requirement for intent should be expressly noted in the provisions themselves, to avoid the appearance of penalising accidental omissions or errors.

Section 57(2) – consent to copy or record details on the Access Card

64. Section 57(2) allows for the copying or recording of the access card number, photograph or signature with the written consent of the owner of the Access Card. The Office notes that permitting individuals to be able to consent to the access card number being recorded is inconsistent with the terms and policy intent of National Privacy Principle 7. A provision of this type is likely to raise significant privacy risks in the medium to long term and may undermine the trust that the community has in the access card proposal.

65. While generally, providing consumer control over their personal information is consistent with good privacy practice, the Office considers that a consent mechanism is unlikely to be appropriate for a government issued unique identifier that will be held by most of the adult population. By way of contrast with other government issued identifiers, a consent mechanism is not available for the handling of the Tax File Number.

66. The Office's concerns about providing this consent mechanism are due to the fact that the privacy risks of sharing unique identifiers are not always immediate. The risks accumulate as more organisations or agencies come

to adopt the number, and as greater amounts of personal information become associated with that number. Accordingly, individuals may not always be aware of the potentially significant long term privacy risks when asked to consent to such handling, especially where they may be offered an immediate and tangible convenience.

67. In addition, the Office has previously noted that, in some circumstances, consent to a particular information handling practice may be an imperfect form of privacy protection. This is most evident in the case of "bundled consent", that is, the bundling together of consent to a wide range of uses and disclosures of personal information, without giving the individual the opportunity to choose which uses and disclosures they agree to. Bundled consent is often sought as part of the terms and conditions of a service.

68. The Office suggests that organisations should not be permitted to copy or record the Access Card number with the individual's consent, unless it is in accordance with a requirement of other legislation. An example of this may be the *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006, which directs the organisation to keep a record of the information that a person has provided to identify themselves. With this exception, in relation to the Access Card number, the Office believes that the Bill should reflect the requirements and protections in National Privacy Principle 7, which are aimed at preventing organisations from adopting, using or disclosing Commonwealth issued identifiers.

Part 5 – Miscellaneous

Division 2 – Identity guidelines

69. The "identity guidelines" under section 66 hold considerable significance for the manner in which the Secretary and delegates make important decisions under the Bill, including how an individual may prove their identity, their eligibility for registration, and the issuing of the access card.

70. The Office welcomes these potentially crucial guidelines being subject to Parliamentary scrutiny. In addition, the Office suggests that they be subject to mandatory consultation, including with the Privacy Commissioner. This importance is heightened given the need to ensure that they are consistent with other Australian Government identity management initiatives.

Division 3 – Delegations and authorisations

71. In relation to powers of the Minister which can be delegated under section 68(2) and are to be exercised by legislative instrument, the Office believes there may be benefit in clarifying that these functions will continue to receive the benefit of parliamentary scrutiny when delegated.

72. For example, as the Office understands it, item 17(b) of s 17 may be delegated to the Secretary (determining what additional information may be stored on the register). However, it is noted that section 17(2) states that the Secretary's determinations under item 17 (which would ordinarily relate to administrative matters under item 17(a) of s 17) are not legislative instruments. The Office assumes that where a power is to be exercised

subject to parliamentary oversight, that oversight remains if the power is delegated. The Office suggests this should be articulated in the legislation.

Possible matters for future legislation

73. The Office looks forward to opportunities for public comment on future legislative proposals that affect the access card system, particularly the second tranche of dedicated legislation.

Determining future uses

74. The Office acknowledges the role of the objects and purposes clauses in providing guidance on how the access card system may be used, and welcomes the legislative oversight which would need to accompany the amendment of those clauses.

75. However, some provisions of the Bill, such as the object in s 6(c) on fraud reduction and the interpretation of s 7 in the Explanatory Memorandum to incorporate fraud minimisation as part of the purpose of providing the benefits to the appropriate individuals, may leave open the prospect of a broader interpretation of possible uses than that which the public might reasonably expect. It does not appear that the Bill currently expressly proscribes uses other than uses for the purpose articulated in s 7.

76. The Office believes that legislation should prescribe, in detail, a statutory process for assessing and approving any future uses of the access card and associated systems (such as the register). It is suggested this would positively impact on public confidence in the initiative.

77. The statutory process could be applied to proposed uses, whether or not those uses fit within the current objects and purposes. They could also apply to any proposed expansion of the objects and purposes.

78. Appropriate mechanisms could include a combination of mandatory public consultation; parliamentary committee review; referral to an independent panel of experts; and review by the Privacy Commissioner. Ultimately, any future uses should be subject to parliamentary oversight and amendment to primary legislation.

79. While such detailed processes are not included in the Bill, the Office looks forward to the opportunity for public comment on such proposals in the second tranche of legislation.

Specific secrecy provisions

80. The Office notes the role of the *Privacy Act 1988* as a source of underlying privacy protection for the access card system. However, the size and scope of the register raise privacy risks that the Office believes requires additional privacy and secrecy protections to be enacted in legislation. Such legislation could also ensure uniform protections over all entities that may use the access card and associated systems, including in regard to acts and

practices of individuals and companies not currently within the Privacy Act's jurisdiction.

81. The Office recommends the development of specific secrecy provisions for the second tranche of legislation to protect the personal information contained in the register and the card chip.

82. This is particularly important given the size, sensitivity and coverage of the access card databases. As previously noted, this would be the first biometrics-enabled database established for the majority of Australia's adult population (containing a biometric photograph, a digitised signature, and a large amount of other personal information).

83. Such provisions would provide greater protection to personal information held on the register and the access card chip, over and above existing legislation such as the Privacy Act, which does not apply to the activities of individuals, small businesses and state or territory government agencies, and does not provide for criminal sanctions.