Australian Government

Office of the Privacy Commissioner

Consultation on Australian Government Smartcard Framework; Smartcard Implementation Guide – Part d (Working Draft Version 2.0)

Submission to Australian Government Information Management Office

May 2007

GPO Box 5218 SYDNEY NSW 2001 • Privacy Hotline 1300363992 • www.privacy.gov.au

Office of the Privacy Commissioner

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

The Office welcomes the opportunity to provide comments on Part d of the Australian Government Smartcard Framework ("the Framework"), the *Smartcard Implementation Guide* ("Part d").[1] Our comments make specific reference to Part d/1 and d/2. The Office has previously made a submission on Part C of the Framework in April 2007[2], and on the Draft Smartcard Framework in March 2006[3], and welcomes the attention that has been paid to privacy issues by the Australian Government Information Management Office ("AGIMO") during development of the Framework.

The Office recently made a submission to the Australian Law Reform Commission's ("ALRC") *Inquiry into the Privacy Act*.[4] Chapter 11 addresses developing technologies, and makes some comments about smartcards.

The Office notes that Part d/1 provides guidance on developing a business case where a smartcard is a proposed solution to an identified business need. It is stated to be complementary advice to a more general publication, the ICT Business Case Guide, published by AGIMO in September 2006,[5] and deals specifically with issues that may be encountered in relation to smartcards.

The Framework provides a collated source of guidance for agencies considering a smartcard project, highlights important issues to be considered and addressed, and identifies important privacy issues which should contribute to the overall success of a smartcard project.

The Office particularly welcomes the reference to privacy obligations throughout Part d including the different jurisdictions and particular sectors, the inclusion of explanations of personal information and sensitive information,

[1] Available in four parts at http://www.agimo.gov.au/infrastructure/smart_cards/release_for_comment [accessed 30 April 2007].
[2] Submission available at http://www.privacy.gov.au/publications/sub_agimo_010507.doc
[3] Submission available at http://www.privacy.gov.au/publications/Smartcardsub020506.pdf
[4] Submission available at http://www.privacy.gov.au/publications/alrc280207.html
[5] AGIMO ICT Business Case Guide available at http://www.agimo.gov.au/government/the_ict_investment_framework/business_case_tools_and_review

and the recommendation that consideration of privacy issues be an early step in a smartcard implementation.[6]

Is a smartcard solution appropriate?

Part d/1 deals with developing business cases for smartcard projects. The Office welcomes the requirement in Part d for detailed and documented consideration of the identified business need, and the guidance regarding assessment of potential solutions. In particular, the Office welcomes the advice that agencies consider the potential impact on stakeholders in addition to whether the proposal will address the identified problem, and a comparative cost-benefit analysis of potential solutions.[7] This approach is similar to that previously recommended by the Office in the submission regarding the Health and Social Services Access Card.[8]

The assessment and evaluation of proposals suggests comparison of options against a "Do Minimum" option.[9] Given the potential complexities, costs and risks involved in implementing a smartcard solution, the Office welcomes the Framework's recognition of the importance of considering whether a smartcard is the most appropriate solution, and whether a simpler or lower cost technology may achieve the desired results.

Privacy – constraint or benefit?

Part d of the Framework includes references to privacy as both a potential constraint and as a potential benefit arising from a smartcard proposal. The Office considers that it is appropriate that compliance with privacy regulation is identified as a constraint,[10] as all smartcard projects will need to be aware of and comply with the privacy legislation or regulation relevant to the particular jurisdiction. Such compliance is likely to accord with community expectations and promote trust in the smartcard.

It is also useful to consider the potential for smartcards to enhance privacy.[11] The Office recognises that, when privacy is built in, and information is collected and handled appropriately, smartcards can achieve privacy-enhancing results. Given this, privacy issues should be given due weight and consideration when assessing the impact, costs and benefits of a smartcard proposal.

Holistic security and privacy practices

The Office welcomes the attention paid in Part d/2 to the component parts of a smartcard implementation.[12] It is essential that appropriate security and privacy practices apply to information stored on the physical card, the chip,

[6] See particularly, page 19 of Part d/2
[7] At page 20 of Part d/1
[8] See paragraph 34 at http://www.privacy.gov.au/publications/accesscard_sub_082006.html
[9] See page 21 of Part d/1
[10] See page 40 of Part d/1
[11] See page 45 of Part d/1
[12] For example, page 29 of Part d/2

the card operating system and any other applications, the smartcard readers, and all backend systems that will provide support or functionality to the smartcard.

The Office also supports the Framework's multi-faceted approach to ensuring privacy is incorporated into smartcard projects, including privacy-enhancing technology measures to complement policy and legal measures to protect privacy.[13] Usefully, specific mention is given to agencies considering the need for dedicated legislation to regulate the privacy management of the smartcard.[14]

Interoperability

The Office considers that interoperability should be limited to where it is necessary for the intended scope of the proposed smartcard operation, rather than building in interoperability as a future contingency. The Office supports the recommendations that an assessment be made regarding whether interoperability is a requirement for a particular smartcard project,[15] and further, that where interoperability is considered necessary, that a Community of Interest be identified to establish how much interoperability is necessary in the circumstances.[16] Later, reference is again made to establishing interoperability with other systems "as required".[17]

Part d/2 refers to "blended functionality", which refers to using a smartcard and the supporting infrastructure for two or more unrelated purposes.[18] The Office suggests that, particularly if the smartcard contains personal information, and where the purposes are completely unrelated, then it may not be appropriate to share a smartcard. However, the Office welcomes the statement that wherever possible, clear technical isolation should be implemented between the intended functions.

The Office has provided more detailed comments regarding interoperability in its submission on Part C of the Framework.[19]

User Acceptance

Part d recognises the importance of user acceptance to the successful implementation of a smartcard.[20] This is also apparent in discussions regarding education and user awareness of the smartcard project.[21]

[13] See pages 45 and 54 of Part d/1, This accords with the Office's comments on the Health and Social Services Access Card, from paragraph 15 at http://www.privacy.gov.au/publications/accesscard_sub_082006.html
[14] See Pages 22 and 97 of Part d/2
[15] Page 41 of Part d/1
[16] Also at page 23 of Part d/2
[17] At page 23 of Part d/2
[18] See page 104 of Part d/2
[19] See footnote 2 for link to submission
[20] See pages 47 and 53 of Part d/1, with regard to biometrics, at page 9 of Part d/2, and at pages 26, 49 and 113 of Part d/2 in relation to the risk of damage to public trust.
[21] See, for example, at page 57 of Part d/1 and at page 22 of Part d/2

Appropriately trained staff contribute to achieving user acceptance. Staff should be familiar with the operation of the smartcard, and be able to answer questions and concerns of smartcard users, particularly regarding privacy issues and security of information associated with the smartcard.[22]

Compliance with legal safeguards and statutory requirements, particularly with regard to privacy, is identified as a critical factor, as even appearance of compromising on these matters may undermine user acceptance.[23]

The Office supports the Framework's close attention to issues of user confidence and support of any smartcard implementation.

Information on the Face of the Card

Part 18 of Part d/2 deals expressly with user acceptance, and encourages smartcard implementation to facilitate, where possible, individual choice regarding their engagement with the smartcard, including aspects such as choice of preferred name or pseudonym on the face of the card.[24]

Part d provides a discussion of the information that should be shown on the face of the card. It states that "in general, agencies should avoid printing too much information on the surface of the card"[25] and that "each element added to the front and/or the back of the card should be able to be justified on the basis of the functionality or business process it is enabling"[26]. As a general principle, this approach should result in better privacy practice, and reduce concerns regarding user acceptance.

Part d states that the inclusion of a photo on the face of the card should only be permitted where there is an actual need for that means of cardholder identification, such as cases of employee identification, or drivers licences.[27] This section also suggests that printing a name on the face of a smartcard should only occur if it serves a purpose. Part d recognises that there may be smartcard systems which would not require any personal identifiers on the card, or the chip, such as cards used in transit systems.

The Office welcomes this approach, and supports the provision of individual control, where possible, over the information that is recorded on the face of the card.

Privacy Impact Assessments

The Office welcomes the inclusion of references in Part d to Privacy Impact Assessments (PIA).[28] In particular, it states that the handling of personal information is a "crucial policy and technology objective for a smartcard

[22] Including at page 58 of Part d/1
[23] See page 47 of Part d/2
[24] From page 112 of Part d/2
[25] See page 69 of Part d/2
[26] See page 65, and also page 69 of Part d/2
[27] See page 67 of Part d/2
[28] See page 52 of Part d/1; pages 18, 40 and 49 of Part d/2

scheme"[29], and that "it is accepted best practice for any program that deals with personal information to undertake one or more Privacy Impact Assessments" in accordance with the Office's Privacy Impact Assessment Guide.[30]

However, the Office notes that merely conducting a PIA will not necessarily result in reduced privacy concerns. A PIA may identify areas of privacy concern, but additional steps, such as transparency (allowing stakeholders, including the public where appropriate, to read the PIA report) and taking action on the recommendations arising from the PIA, will be needed to effectively reduce any privacy concerns with a smartcard project. This is recognised at page 96 of Part d/2, where is suggests that visible and well resourced attention be paid to PIAs, with proper engagement of the design team so that findings are factored into implementation.

Identifiers

The Office notes that Part d/2 begins by acknowledging that not all smartcards will need to function as identification authentication.[31] However, for those projects where smartcards will function as identification, the Office welcomes the acknowledgement that the use of identifiers raises particular privacy issues "especially… when unique identifiers are issued to large groups of cardholders and the identifier is used by many relying parties in multiple domains".[32]

Later in Part d, it states that "there may be privacy risks associated with printing of unique number on the face of the cards. Especially in scenarios where the card is used many times by various agencies and other relying parties, the card number may become a de-facto identity number for the cardholder".[33]

The Office considers that it is important that such risks are highlighted in this Framework, and considers that alerting agencies to the risk of creating an identity number, or identity card, will ensure that the risk is given due consideration in the planning of any smartcard project. The Office discussed the privacy risks of unique multi-purpose identifiers in Chapter 12 of it's submission to the ALRC *Inquiry into the Privacy Act*.[34]

The Office also notes that Part d alerts agencies to the choice between persistent identifiers and identifiers that are renewed with each card, and indicates that privacy may be better protected by use of identifiers that change periodically. The Office acknowledges that while this may be a better option than a lifetime identifier, in some circumstances, particularly where the

[29] At page 96 of Part d/2
[30] The Office's Privacy Impact Assessment Guide is available at http://www.privacy.gov.au/publications/pia06/index.html
[31] At page 2 of Part d/2
[32] See page 18 of Part d/2
[33] See page 67 of Part d/2
[34] See chapter 12 – Submission available at http://www.privacy.gov.au/publications/submissions/alrc/c12.html

smartcard is intended to be widely used, it may not adequately mitigate the risks associated with a unique identifier. It may be useful to note this in Part d, and indicate that in such cases, other mitigation methods should be used to reduce the risk of creating a universal ID number.

Access controls and sensitive information

Practices which result in the minimum amount of information being collected and stored on a smartcard or chip, and which restrict access to information based on what a party needs to know, are likely to minimise the privacy risks to the information. Part d supports this, and in particular, cautions that failure to take these steps may impact upon compliance with privacy law.[35]

Part d makes specific comments that a smartcard system should incorporate access controls, such that the person, or reader, that is trying to access information on the chip, or back end systems, is authorised to see that information.[36] The Information Privacy Principles and the National Privacy Principles require agencies and organisations respectively to take reasonable steps to secure the information they hold. Where a smartcard contains or acts as a link to sensitive information, such 'reasonable steps' are likely to constitute robust security measures. These measures may include access controls such as mutual authentication to ensure that the reader is appropriately authorised to access information linked to a particular card.

Part d also alerts agencies that smartcards may contain sensitive information, and that different security arrangements may need to be made for sensitive information, compared with "non sensitive information that is allowed to be read by anyone".[37] The Office notes that sensitive information is a term defined in the Privacy Act, however, in practice, different people may consider different types of information sensitive. For example, some people may consider their residential address to be sensitive information, such as in the case of domestic violence, and others may consider their gender to be sensitive information, such as transsexuals. Where an agency or an organisation requires a contact address, an individual may choose to provide a PO Box, and unless there is a particular reason that a residential address is required, the individual should be afforded the choice.

Registration and synchronisation of information

The Office notes the discussion of data quality and the use of data cleansing and updating techniques, and data synchronisation, particularly where a smartcard facilitates interoperability between agencies. An example is offered of a cardholder who updates certain information, such as an address, with one agency, and Part d suggests that this information may need to be distributed to all involved agencies to avoid data inconsistency.[38]

[35] See page 26 of Part d/2
[36] See page 15 of Part d/2
[37] Pages 13 and, with regard to sensitive information and risk management, at 47 of Part d/2
[38] See page 55 of Part d/2

The Office considers that there may be legitimate reasons for a person to record different information, such as different addresses, with different agencies. An example may be where a resident of a rural community is required to move to a city temporarily, such as for a hospital stay of a relative or for a course of outpatient treatment. An individual may need to be contactable at the city address for their dealings with certain agencies, but wish to retain their home address for their dealings with other agencies. Automatic synchronisation of information limits the ability for an individual to tailor their interactions with agencies as appropriate for their circumstances.

Function creep

There is recognition in Part d that scope creep could impair the success of a program[39] and that "designers should refrain from introducing scope creep unless there is a proven business need".[40] The Office understands that scope creep involves expanding the functionality of the smartcard, at the design stage, beyond the initial business case, and considers that this raises similar issues to function creep, which generally involves incremental expansion in the purpose for which a system or object is used. In both cases, the smartcard may be employed for purposes that were not initially agreed to or envisaged. One way to limit the risk of function creep is to provide for a specific process, incorporating elements of transparency, consultation, independent review and parliamentary oversight where appropriate, to manage the introduction of new uses for a smartcard.

Additional comments on the risks of function creep can be found in the Office's first submission on the Health and Social Services Access Card.[41]

Security

The Office welcomes the attention paid to ensuring appropriate security of smartcard systems, and the information they contain. At page 4 of Part d/1 it states "In the context of smartcards, technology may be able to improve identification and authentication processes of individuals…, increasing the level of information security". It is not immediately clear that improvement to identification will necessarily increase the level of information security. The Office suggests the use of the words "*which may in turn* increase the level of information security".

The Office also welcomes the discussion of the various methods to enhance security to the face of card[42], noting that it can be easily read and copied[43], and to the chip and applications on the chip, particularly a contact-less chip, where, if there is insufficient security, the information can be easily accessed[44].

[39] See page 114 of Part d/2
[40] See page 108 of Part d/2
[41] Available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html
[42] See page 10 of Part d/2
[43] See page 11 of Part d/2
[44] See page 12 of Part d/2

IPPs and NPPs

In certain sections of Part d, reference is made to the National Privacy Principles (NPPs). The Office takes this opportunity to clarify that where Part d is referring to the obligations of *agencies* covered by the Privacy Act, the relevant obligations are the Information Privacy Principles (IPPs). The NPPs, which govern the information handling practices of organisations in the private sector, may be relevant where a smartcard is intended to be used in the private sector. Where a private sector organisation is a contracted service provider to a Commonwealth agency, that organisation will be subject to both the IPPs and the NPPs.[45]

[45] See in particular, the last sentence on page 3 of Part d/1, and potentially the comments on page 96 of Part d/2, though this section may relate to both public and private sector entities.