APPENDIX E

Jurisdictional Report for Australia

CONTENTS

Context

Australia is a federation of six States and two Territories. The federated nation is formally referred to as a 'Commonwealth' and the adjective used is either 'Commonwealth' or 'Federal'.

Each of the 9 jurisdictions has responsibility for its own public sector. Regulation of the private sector in respect of consumer interests is largely performed by the States and Territories under the 'Fair Trading' banner. For the most part, however, any regulation relevant to privacy is incidental rather than intentional. Some have, however, passed privacy laws that impinge upon both the public and private operators in the health care sector.

Each of the 9 jurisdictions has responsibility for its own public sector, but constitutional powers in relation to the private sector are somewhat complex. The Commonwealth has acted in respect of the private sector generally, and the States and Territories have accepted that jurisdictional claim. Some have, however, passed privacy law in respect of the health care sector, which intersects and may conflict with the federal law.

The remainder of this document is structured into sections for the federal government and each of the six States and two Territories, in the conventional sequence of largest-first.

Research

The report has been compiled from the author's knowledge and considerable archival data, the resources provided by the Australian Privacy Commissioner and the Australian Privacy Foundation, information provided by the relevant organisation in each jurisdiction, and research using the Web.

Resources include:

"Privacy Protection Agencies", Australian Privacy Foundation.
Privacy Laws: States and Territories of Australia, Australian Privacy Foundation; and "State and Territory Privacy Laws", Office of the Privacy Commissioner of Australia.[1]
This report reflects research variously conducted and updated during July 2007, including interactions with the Commissioners or their nominees in Victoria, N.S.W. and the Northern Territory, with the Tasmanian Ombudsman, with the Privacy Committee of South Australia and with the Human Rights Unit of the Australian Capital Territory's Department of Justice and the Attorney-General.

[1] at respectively: http://www.privacy.org.au/Resources/Contacts.html#GovP, http://www.privacy.org.au/Resources/PLawsST.html and http://www.privacy.gov.au/privacy_rights/laws/.

I. Australia, Federal Government

Context

This report reflects research variously conducted and updated during July 2007, including an interview with the Australian Privacy Commissioner's nominee, Andrew Solomon, Director of Policy.

Legislative and Policy Framework

Legislation

In 1988, the *Privacy Act* (Cth)[2] was passed, to regulate the federal government public sector.

In 2000, substantial amendments were passed, applying a somewhat different regime to the private sector.

The 1988 Act created a statutory appointment called the Privacy Commissioner, supported by the Office of the Federal Privacy Commissioner (OFPC).[3]

Privacy Impact Assessment (PIA) Guidance Material

The Office released a *Privacy Impact Assessment Guide* for Australian Government and Australian Capital Territory Government agencies in 2006[4].

The Guide was devised so as to provide a brief, high-level overview, and a sense of the main methodology, but with 'drill-down' features such as checklists, in order to ensure it is sufficiently comprehensive. Key features of the Guide are outlined in Appendix 1.

The Guide was designed as guidance for government agencies. However, it is considered by the OFPC to be readily adaptable to apply to private sector companies, and the Office intends to do this, subject to resource availability.

There is no legal obligation on either government agencies or corporations to conduct PIAs (although, as discussed below, that may be changing). It is merely a Commissioner Recommendation. The Commissioner's communications with agencies and the private sector routinely contain segments of text along the following lines: 'The Office suggests that a privacy impact assessment be undertaken as part of the further development of the proposal'.

The Australian PIA

History and Development of the Australian PIA

As early as 1990, there was a clear predecessor to the concept of a PIA in the form of the 'Program Protocol' applied to data matching programmes. The then Commissioner, Kevin O'Connor, the then Deputy Commissioner, Nigel Waters, were successful in submitting to the Parliament that a particularly large 'Parallel Data Matching Program' needed to be subject to a statutory requirement to undertake a prior, justificatory study, and document the specifications for the programme.

---

[2] http://www.austlii.edu.au/au/legis/cth/consol%5fact/pa1988108/

[3] Learn more about the Commissioner and the Office at http://www.privacy.gov.au/ and http://www.privacy.gov.au/about/index.html.

[4] August, 2006. The Guide is available at http://www.privacy.gov.au/publications/pia06/index.html

The requirements of the 'Program Protocol' are declared in Schedule 1 to the Data-Matching Program (Assistance and Tax) Act 1990,[5]

Building on the 1990 'Program Protocol', the then Commissioner, Kevin O'Connor, published Guidelines for 'Data-Matching in Commonwealth Administration' (June 1992). These are not legally binding, but it was recommended that all agencies conduct such an assessment when considering undertaking any form of data matching. The current version is dated February 1998.[6]

The earliest mentions of the term 'PIA' found in Australian sources appear to be the following:

- a 1995 acknowledgement by the Telecommunications Industry Ombudsman that PIAs had a role to play (referred to in the 1997 paper discussed below);
- 1996 papers by Blair Stewart (New Zealand's Deputy Privacy Commissioner), in Privacy Law and Policy Reporter;[7]
- a 1997 call by the Communications Law Centre for implementation of PIAs, invoking Blair Stewart's definition as "a process whereby a conscious and systematic effort is made to assess...any actual or potential effects that [an] activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated" and referring also to David Flaherty's work in British Columbia; [8] and
- papers of Roger Clarke in 1997-99.[9]

In December 2001, the then Commissioner, Malcolm Crompton, issued 'Guidelines for Agencies using PKI to communicate or transact with individuals':[10] These included as Guideline 3:

> "Agencies should undertake a Privacy Impact Assessment before implementing a new PKI system or significantly revising or extending an existing PKI system".[11]

A PIA was depicted as "a method of identifying privacy risks so that these can be highlighted and addressed when ... systems or ... business applications are being designed, implemented, revised or extended. A PIA may be part of a larger risk assessment and management procedure. Properly done, this assessment will include an understanding of which parties will bear what risks".[12]

It was expressly stated that "agencies should provide their clients with anonymous and pseudonymous options for transacting with them, to the extent that this is not inconsistent with the objectives and operation of the relevant online application"[13]

---

[5] at: http://www.austlii.edu.au/au/legis/cth/consol_act/dpata1990349/index.html and http://www.austlii.edu.au/au/legis/cth/consol_act/dpata1990349/sch1.html.
[6] at: http://www.privacy.gov.au/publications/dmcomadmin.pdf.
[7] at http://www.austlii.edu.au/au/journals/PLPR/1996/39.html and http://www.austlii.edu.au/au/journals/PLPR/1996/65.html.
[8] at http://www.austlii.edu.au/au/journals/PLPR/1997/4.html
[9] at http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.htmland in greater depth at http://www.xamax.com.au/DV/PIA.html.
[10] at: http://www.privacy.gov.au/publications/pki.doc
[11] 'Guidelines for Agencies using PKI to communicate or transact with individuals' p. 29
[12] p. 35.
[13] (Guideline 9, p. 35).

Further guidance was provided on pp. 36-38 (referencing Blair Stewart's work in New Zealand), and a customised checklist for Information Privacy Principle compliance on pp. 39-43.

In January 2003, in a Submission to the Joint Committee of Public Accounts and Audit (JCPAA) on 'Management and Integrity of Electronic Information in the Commonwealth', the then Commissioner, Malcolm Crompton, stated:

> "Recommendation 2 – that Commonwealth agencies be required to undertake privacy impact assessments at the beginning of the development of new proposals and initiatives involving the handling of the personal information of the Australian community.[14]
>
> "These assessments should be published unless national security or law enforcement considerations outweigh the public interest in the publication. If an assessment is not to be published, it should be copied to the Privacy Commissioner, the Attorney-General's Department; the Department of Finance and Administration and the Department of Prime Minister and Cabinet."[15]
>
> and
>
> "Recommendation 3 – that the Cabinet Handbook and the Department of Prime Minister and Cabinet's Drafter's Guide be amended to more specifically guide agencies in their early assessment of the privacy impact of new proposals relevant to Cabinet Submissions, Cabinet Memoranda and like documents".[16]

In November 2004, the Commissioner, Karen Curtis, issued an Exposure Draft of 'Managing Privacy Risk: An Introductory Guide to Privacy Impact Assessment'. The draft was based on considerable research into the experiences of and guidance provided in other jurisdictions, particularly New Zealand, Canada and Ontario. Comment was invited from the public and privacy advocacy groups:[17]

Among other submissions, the Australian Privacy Foundation suggested a number of enhancements. [18]

In August 2006, the final version of the 'Privacy Impact Assessment Guide' was released.[19]

In launching the Guide, the Attorney-General said, "as a matter of good business practice, I strongly encourage government agencies to use the guide to assist them in playing a larger role in promoting privacy compliance".[20]

Completion of PIAs

---

[14] Malcolm Crompton, Submission to the Joint Committee of Public Accounts and Audit (JCPAA) on 'Management and Integrity of Electronic Information in the Commonwealth', at pp. 19-20 of: http://www.privacy.gov.au/publications/jcpaasubs.doc

[15] Ibid, section 3.1.5.1

[16] Ibid.

[17] See Office of the Privacy Commissioner of Australia Media Release, *Announcement: Draft of Managing Privacy Risk - An Introductory Guide to Privacy Impact Assessment for Australian Government and ACT Government Agencies*, at: http://www.privacy.gov.au/news/04_07.html

[18] at: http://www.privacy.org.au/Papers/OFPC-PIA-0502.rtf

[19] at: http://www.privacy.gov.au/publications/pia06/toc.html and http://www.privacy.gov.au/publications/PIA06.doc and http://www.privacy.gov.au/publications/PIA06.pdf.

[20] at: http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases_2006_Third_Quarter_29_August_2006_-_Speech_-_Privacy_impact_assessment_guide_and_layered_privacy_policy_launch

By Which Organisations?

The Privacy Commissioner's 2006 Guide is specifically addressed to government agencies.

PIAs are performed for a wide range of purposes in a wide range of contexts. One particular PIA project utilised several specific features that have the potential to offer considerable payback. Centrelink is the delivery channel for about 100 benefits programmes run by various Australian government agencies. It provides services to over 20% of the Australian population, many of them on a regular basis.[21] The effectiveness and efficiency of Centrelink's business processes are heavily dependent upon use of technology in a manner that works for both the agency and its clients. Automated authentication of clients' voices over the telephone offers considerable promise, but brings with it risks that are not easy to grasp and to articulate.

A number of recent developments show that the Commissioner's 'moral suasion' is having considerable impact:

- since March 2005, the Australian Government Information Management Office (AGIMO – called in other jurisdictions the Office of the Government CIO) has specifically pressed for a PIA to be done in relation to **authentication projects more generally;** [22]
- in June 2006, AGIMO extended the authentication work to the Australian Government Smartcard Framework;[23]

  This requires that "**One or more Privacy Impact Assessments should be undertaken at critical points during the design and rollout of the smartcard solution**, such as at initial design, final design, and whenever a significant change occurs to the deployed system, such as third party agency deciding it may wish to re-use the initial deployment. This is **consistent with the Australian Government e-Authentication Framework**";[24]
- in July 2006, the Privacy Commissioner approved a Biometrics Code prepared by an industry association, the Biometrics Institute.[25] This includes **a requirement for privacy impact assessments as part of the planning and management process for biometrics implementations, which is the first context in which any form of statutory mandation has arisen.** (However, because the code is voluntary and there are virtually no signatories to it, the mandation is currently not meaningful);

[21] at: http://www.centrelink.gov.au/.
[22] See the 'Australian Government Authentication Framework for Business, Part 5 – Evaluating the business, privacy and public policy impacts', at http://www.agimo.gov.au/infrastructure/authentication/agaf_b/impguidegovt/volume3/part5
[23] at: http://www.agimo.gov.au/infrastructure/smart_cards and http://www.agimo.gov.au/__data/assets/pdf_file/56247/Overview_and_Principles_PUBLISHED_June2006.pdf and http://www.agimo.gov.au/__data/assets/pdf_file/56248/Smartcard_Handbook_PUBLISHED_June2006.pdf
[24] fn. 23 at p. a17
[25] at: http://biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8 http://biometricsinstitute.org/associations/4258/files/2006-07%20Biometrics%20Institute%20Privacy%20Code%20approval%20determination%20FINAL.doc

- in April 2007, **the head of the Attorney-General's Department wrote to all agency heads** on privacy issues generally, extolling the benefits of using PIAs early in the project life-cycle;
- **some agencies have implemented internal programmes to apply PIAs**, integrating them with related areas of responsibility. An example is the Department of Defence's 'Fairness and Resolution' Programme;[26]
- since the Guide was launched in August 2006, there have been **23,000 hits or downloads**, with spikes following events such as meetings with agency Privacy Contact Officers (PCOs). Although the OFPC is not directly involved in agency activities, the impression gained by the OFPC is that the Guide is being used quite extensively. It is common for Requests for Tender for consultancy support for PIAs to explicitly require that the Commissioner's Guide be at least reflected, and in most cases complied with. On the other hand, PIAs are not yet performed as a matter of course, even within Government, and even for projects with significantly privacy-invasive features.

Examples of PIAs known to have been conducted by federal agencies include are in Appendix 1.

Examples of PIA Reports known to have been published are listed in Appendix 2.

Private Sector PIAs

There is some degree of application in the private sector, but it is not widespread, and few PIAs have been widely publicised. Whereas the public sector uses the terms 'compliance check', 'privacy notices', 'PIA' and 'privacy audit', the terminology applied in the private sector includes 'privacy strategy', 'privacy (management or implementation) plan', 'privacy policies', 'privacy statements' and 'privacy review'.

In March 2005, the Commissioner, Karen Curtis, published a review of the private sector provisions of the *Privacy Act*. In s.8.4, 'Options for reform', the Report referred to:

> "Promote privacy impact assessments and privacy enhancing technologies: ... **"**The Office could encourage technology developers and implementers to conduct a privacy impact assessment for large scale high privacy risk projects. A wider review of the *Privacy Act* could consider the question of whether the Privacy Act should include provisions which provide for a privacy impact assessment to be carried out in specified circumstances."[27]

It is understood that in 2006 Coles-Myer[28] adapted the Commissioner's PIA Guide to reflect the private-sector National Privacy Principles (NPPs) rather than the public-sector Information Privacy Principles (IPPs), and applied them to a project to produce a customer data warehouse.

Examples of PIAs known to have been conducted in the private sector, in public-private partnerships, or otherwise with considerable private sector involvement are listed in Appendix 3.

Who Writes and Participates in Development of PIAs?

[26] at: http://www.defence.gov.au/fr/ and http://www.defence.gov.au/fr/Privacy/privacyimpact.htm
[27] (pp. 255-256) http://www.privacy.gov.au/act/review/revreport.pdf.
[28] Australia's largest retailer, with more than 1900 stores throughout Australia and New Zealand, at: http://www.colesgroup.com.au/Home/.

The Guide proposes that agencies adopt a team approach, using 'in-house experts' and outside expertise as necessary. In practice, there has been considerable use of the small number of specialist consultants with expertise in the area.

When?

The Guide implies that PIAs should be commenced early, in order to shape the evolution of the project. It provides only limited guidance as to how to assess when a PIA is needed. It does, however, refer to "significance", "size", "complexity" or "scope", the extent to which the project involves "collection, use or disclosure of 'personal information'", both in general, and particularly "information that is generally regarded as sensitive".

External Consultation

Centrelink formed a PIA Consultative Group (PCG), comprising representatives of people in various client segments, together with advocates for consumer and privacy interests. Project staff provided background information and briefings to the PCG, enabling members to surface and articulate concerns. By working with such a group, an agency's officers can achieve much deeper insight into the project's likely negative impacts, and what can be done to avoid or ameliorate them. In extreme cases, advance warning could be gained of serious public sensitivities.

The PCG was called together in several successive phases of the project. Briefings became shorter and conversations more tightly focused. The confidence of the PCG members in the agency's goodwill was greatly increased as they found that the subsequent phases were clearly reflecting the outcomes of earlier rounds.

Another approach adopted by Centrelink (in a project to develop an 'authentication hub' to enable single sign-on to multiple agencies) was to expose the design to people from various client segments who would be affected by the project. Consumer/citizens are seldom able to discuss abstract ideas, so a prototype was essential to enable this form of consultation to be effective. Deeper understanding about people's views and reactions can be gained by drawing the invitees into focus groups.

These approaches to consultation contribute significantly to risk reduction in complex IT projects. Feedback is captured at multiple stages in the process, which underpins an adaptive approach to system design and avoids new systems being 'legacy systems' even before they are implemented.

Review/Approval of PIAs

The OFPC drew attention to a risk inherent in mandation. Organisations might focus on compliance rather than adopting a strategic approach, and might therefore fail to gain the benefits that are available from appropriately open and imaginative processes. This makes it all the more important for agencies and corporations to be themselves responsible for devising an appropriate process, rather than being subject to overly prescriptive dictates by the Parliament or the Privacy Commissioner.

Public Availability

The Guide envisages that PIA Reports will generally be published. A few have been. See Appendix 3.

Lessons Learned

A number of areas of weakness in PIAs has been commented on by participants and observers. There remains a tendency for agencies to confuse a PIA with a check of compliance with the provisions of the *Privacy Act* or even just the Information Privacy Principles. The use of the small number of consultants with specialist expertise tends to result in PIA processes with broader scope and better ability to deliver benefits to the agency and its clients alike.

The mapping of information flows relevant to privacy impacts has proven to be challenging in some contexts. The documentation needs to be sufficiently full and clear, but also accessible, and this requires skill and effort.

A common shortfall has been a failure to define 'stakeholders' so as to encompass the people affected by the project, and to involve them and/or their representatives and advocates in the PIA process.

Finally, depending on the nature of the project, the scope of a PIA may need to extend beyond information privacy to encompass other dimensions, including privacy of the person (e.g. proposals for the imposition of biometric measurements), privacy of personal behaviour (e.g. visual surveillance) and privacy of personal communications. There may also be benefits for the agency (both in terms of cost-savings and benefit-enhancement) in extending the scope to other social impacts. such as equity, accessibility, anti-discrimination and occupational health and safety.

Directions of PIAs in the Jurisdiction

At this early stage, there has been no formal review of the 2006 Guidelines or their application. The OFPC is, however, looking to review and enhance the Guide during 2008, in what may be by then a somewhat different context. It is not seeking to move towards an approval model, believing that the most effective role it can play is to provide a framework, methodology and tools, and be available to provide high-level advice and review of agencies' PIA plans, while ensuring that the effort is invested (and the benefits are gained) by the organisation sponsoring the project.

In March 2005, the Commissioner's Review of the private sector provisions of the *Privacy Act*, included,[29]

Recommendation 1: The Australian Government should consider undertaking a wider review of privacy laws in Australia to ensure that in the 21st century the legislation best serves the needs of Australia" [30]

Partly in response to that Recommendation, the **Senate Legal and Constitutional References Committee** held an Inquiry into the Privacy Act during the first half of 2005. Several organisations submitted that PIAs should become a requirement under particular circumstances, including the Victorian Privacy Commissioner, the Law Institute of Victoria, the Australian Privacy Foundation, and Electronic Frontiers Australia.

The Committee's Report expressed concern generally, and about several particular projects that used advanced information technologies or were otherwise highly privacy-intrusive. It considered that **"it is possible update the Privacy Act in a 'technology neutral' way to reflect the technological changes that have occurred and to enable the Privacy Act to deal with these new technologies"**. It made general and specific Recommendations to address the situation, including:

Recommendation 5

[29] at: http://www.privacy.gov.au/act/review/revreport.pdf.
[30] At p. 8.

> 7.13 The committee recommends the Privacy Act be amended to include **a statutory privacy impact assessment process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information**.

Relevant excerpts from the Senate Committee's Report are provided in a companion document.

In January 2006, partly as a consequence of the Senate Committee's Recommendations, the Attorney-General provided terms of reference to the Australian Law Reform Commission to conduct a Review of the operation of the *Privacy Act*.

In October 2006, the Commission published a substantial Issues Paper, which discussed the question of PIAs, and asked the following specific questions:

> **Question 6–6:** Should the *Privacy Act* require a privacy impact assessment to be prepared for:
>
> (a) all proposed Commonwealth legislation;
>
> (b) other proposed projects or developments of agencies; or
>
> (c) other proposed projects or developments of organisations?
>
> **Question 6–7:** If privacy impact assessments are required:
>
> (a) who should be involved in preparing the assessments;
>
> (b) who should be entitled to view the results of the assessments;
>
> (c) who should bear the cost of the assessments; and
>
> (d) what role should the Privacy Commissioner play in overseeing any requirements placed on agencies or organisations in this regard?

Relevant excerpts from the Issues Paper are provided in a companion document.

A number of Submissions are known to have been made in response to these questions, and it is generally assumed that agencies and industry associations may have made Submissions as well, which the ALRC does not publish and which the organisations concerned may well not publish either.

In March 2007, in the Executive Summary of the Commissioner's Submission to the Australian Law Reform Commission's Review of Privacy - Issues Paper 31, the Commissioner recommended that "public sector agencies be required to undertake Privacy Impact Assessments for new projects or legislation that significantly impact on the collection or handling of personal information".

More specifically, the Privacy Commissioner submitted, “The Office supports the introduction of a statutory requirement on public sector agencies to undertake a Privacy Impact Assessment (PIA) for new projects and/or legislation that significantly impact on the collection or handling of personal information. This should include:

- a set of criteria to establish when a PIA is required;
- an appropriate regulatory mechanism to ensure compliance.

2. The Office does not believe a mandatory requirement should be imposed on private sector organisations to undertake a PIA. However, organisations should be encouraged to undertake a PIA for large scale, high privacy risk projects.

3. **The Office should develop PIA guidelines tailored for the needs of the private sector through consultation**." [31]

Trends

In interview, the OFPC felt that momentum towards more widespread use of PIAs was building, in both the public and private sectors.

[31] at: http://www.privacy.gov.au/publications/submissions/alrc/exec.html#Question44

Appendix 1: Key Features of the Australian PIA Guide

- It is specifically **addressed to government agencies**. The Privacy Commissioner has separately flagged the need for, and the intention to deliver, PIA Guidelines for the private sector;
- It introduces the concept of a PIA by saying it "**'tells the story' of a project or policy initiative from a privacy perspective** and helps to manage privacy impacts" (p. 4), and ascribes that depiction to David Flaherty;
- It defines a PIA as "**an assessment tool** that describes the personal information flows in a project, and analyses the possible privacy impacts that those flows, and the project as a whole, may have on the privacy of individuals" (p. 4) – re Q3;
- It frames the purposes of doing a PIA, and the benefits arising from it, in terms of **the assistance a PIA can provide to agencies**. The approach is well summed up by the catch-phrase "The PIA pay off: helping to ensure the success of the project" (pp. 4-5, 7);
- It stresses the **risk management aspects** of a PIA (pp. 5-7), and in doing so refers to the relevant section of the Ontario Guidelines (1999, pp. 15-16);
- It **clearly distinguishes a PIA from privacy law compliance**, referring to the need for the agency to consider the "values the community places on privacy – trust, respect, individual autonomy and accountability – and to reflect those values in the project by meeting the community's privacy protection expectations" (pp. 5-6) – re Q3;
- It focusses on **process rather than product**: "A PIA works most effectively when it forms part of a project's development, so that it helps to shape the evolution of the project. This ensures that privacy is 'built in' rather than 'bolted on';
- "Given the importance of a PIA in the evolution of a project involving personal information, the PIA document itself will also usually tend to be an evolving or living document. ... **Projects which are more significant in scope may even require more than one PIA throughout their development**" (p. 7);
- It asks the question "Is a PIA Necessary?", and refers to '**Threshold Assessment**' (p. 10). The Privacy Commissioner provides only limited guidance as to how to assess that Threshold, but it does refer to "significance", "size", "complexity" or "scope", the extent to which the project involves "collection, use or disclosure of 'personal information'", both in general, and particularly "information that is generally regarded as sensitive" (p. 8) – re Q4;
- It proposes **"a team approach"**, using "various 'in-house experts'" and "outside expertise as necessary". "In many cases, a set of 'fresh eyes' looking over a project can identify privacy impacts not previously recognised" (p. 8) – re Q5;
- "It will often be appropriate to consult widely. **Consultation with key stakeholders is intrinsic to the PIA process** as it helps to ensure that key issues are noted, addressed and communicated. As a PIA also involves consideration of community attitudes and expectations in relation to privacy, and because potentially affected **individuals are likely to be key stakeholders, public consultation will also often be important**" (p. 9) – re Q6;
- "The PIA should **feed into** further planning about the project's next steps", including resource allocation, stakeholder management, advising Ministers and

government (including about risks), staffing, **the design of the scheme**, trialling, testing, consultation, public education and evaluation (p. 17);

- It envisages that the results, in the form of **the PIA Report, will be published** (p. 17) – re Q7. In interview, the OFPC noted that, where a multi-phase PIA process is conducted, there may be advantages in early documents not being published, in order to help discussions to be open, and ideas to 'gel';
- Guidance is provided in relation to the **conduct of the PIA**:
  - project description (p. 13 and Module B);
  - mapping the information flows (p. 14 and Module C);
  - privacy impact analysis (pp. 15-16 and Module D);
  - Information Privacy Principle compliance (Module E);
  - privacy management, recommendations, implementation, and post-implementation review (pp. 16-17 and Module F);
- Because the statute does not mention PIAs, and the Office is not resourced to provide anything more than general assistance to agencies, **the Privacy Commissioner has no formal role** in the development, endorsement or approval of PIAs (p. 17) – re Q5, Q8;
- "It is important to note ... that, whilst information privacy is the regulatory focus of the Office and this Guide, it is only one aspect of privacy more broadly. For example, there are other types of privacy (such as bodily privacy; territorial privacy; communications privacy).1 **Whilst this Guide is primarily designed to address information privacy issues through the PIA process, other types of privacy can also be considered, particularly where such privacy issues may pose risks to the overall success of the project**" (p. 3).

Appendix 2: Examples of PIAs by or for Australian Government Agencies

- National E-Health Transition Authority (NEHTA), re a unique health identifier (2006-07)
- Access Card Privacy and Consumer Task Force, re a proposed national identification scheme (2006-07)
- Attorney-General's Department, re Document Verification Service (DVS, 2007)
- Attorney-General's Department, re AusCheck – employee background checking services for the maritime and aviation industries (2007)
- Centrelink (the government benefits administrator), re a voice authentication scheme to be implemented within the IVR application on the (very) high-volume call centre (2005, 2006, 2007)
- Australian Communications and Media Authority (ACMA), re ENUM (a scheme to enable mapping between telephone numbers and Internet IP-addresses (2006)
- Attorney-General's Department, re provisions within the Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules (AML-CTF, 2006)
- Department of Health, in relation to Electronic Health Records (2006)
- Australian Government Information Management Office (AGIMO), re the Australian Government Authentication Framework (AGAF, 2004, 2005, 2006)
- Australian Government Information Management Office (AGIMO), re the Gatekeeper PKI Framework (2006)
- Department of Human Services, re a common login-point for multiple client-facing agencies (2006)
- Attorney-General's Department, re provisions within a money-laundering / counter-terrorism Bill (2006)
- Department of Human Services, re a proposed ID card for clients of a variety of agencies (2005)
- Department of Employment & Workplace Relations, re Workplace Reform (2005?)
- Department of Education, Science & Training, re a Learner Identity Management Framework, a Commonwealth-State collaboration featuring a unique student identifier (2005)
- Australian Bureau of Statistics (ABS), re enhancements to the 2006 Census (2005)
- Department of Health, re electronic consent (2004)
- National Office of the Information Economy (NOIE), re the Australian Government Authentication Framework (AGAF, 2003)
- Centrelink, re a proposed ID card for Centrelink clients (1998)
- Department of Workplace Relations and Small Business, re a business register (1998)
- Australian Commission for the Future, re smartcard payment schemes (1996)

Appendix 3: Examples of Published PIA Reports by or for Australian Government Agencies

- NEHTA Unique Health Identifier (Privacy 'Blueprint' rather than PIA), at http://www.nehta.gov.au/index.php?option=com_docman&task=doc_details&gid=148

- Attorney-General's Department, re Document Verification Service (DVS, 2007), at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(756EDFD270AD704EF00C15CF396D6111)~FINAL+PIA+for+publication+on+webpage+-+June+2007.pdf/$file/FINAL+PIA+for+publication+on+webpage+-+June+2007.pdf

- Attorney-General's Department, re AusCheck – employee background checking services for the maritime and aviation industries (2007), at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(756EDFD270AD704EF00C15CF396D6111)~Privacy+Impact+Assessment+-+Auscheck.pdf/$file/Privacy+Impact+Assessment+-+Auscheck.pdf

- Attorney-General's Department, re provisions within the Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules (AML-CTF, 2006), at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~88Privacy+impact+assessment+aml-06.pdf/$file/88Privacy+impact+assessment+aml-06.pdf

- Australian Government Information Management Office (AGIMO), re the Gatekeeper PKI Framework (2006), at http://agencysearch.australia.gov.au/search/click.cgi?url=http://www.agimo.gov.au/__data/assets/pdf_file/52237/Galexia_Privacy_Impact_Assessment.pdf&rank=3&collection=agencies

- Australian Bureau of Statistics (ABS), re enhancements to the 2006 Census (2005), at www.abs.gov.au/websitedbs/D3110124.NSF/f5c7b8fb229cf017ca256973001fecec/fa7fd3e58e5cb46bca2571ee00190475!OpenDocument

Appendix 4: Examples of Private Sector PIAs

- Coles-Myer, re a customer data warehouse (2006)
- Telecommunications, specifically ENUM, undertaken by a Working Group coordinated by the regulator (ACMA), but also involving industry associations and some technology providers (2006)
- An identity management service (Fasfind, 2004)
- Transport ticketing (Melbourne myki, 2004)
- Forensic applications of an email archive analysis product (Nuix, 2002)
- A PKI certificate authority for the health sector (Healthexchange, 2000)
- Toll-roads (Melbourne CityLink, 1998)

Appendix 5: Senate Legal and Constitutional References Committee Inquiry into the *Privacy Act* 1988

Context

In December 2004, the Legal & Constitutional References Committee of the Australian Senate was given a reference to conduct a Review Of The *Privacy Act* 1988:
http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/tor.htm

The 49 published Submissions are at:
http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/submissions/sublist.htm

In June 2005, the Committee published its Report, entitled 'The real Big Brother: Inquiry into the *Privacy Act* 1988'. The document is at:
http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/report/index.htm
http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/report/report.pdf
(800KB)

This document identifies all parts of the text that use the term 'privacy impact assessment', and provides excerpts of them. Segments of particular significance are highlighted in bold-face type.

Excerpt 1

Privacy impact assessments (p. 21-22)

3.25 **Another suggestion put forward in submissions [by the Victorian Privacy Commissioner] was that privacy impact assessments should be conducted prior to the implementation of new technologies.34 The APF submitted that privacy impact assessments are now a mandatory requirement in several jurisdictions including the USA and Canada. Criteria should be developed, drawing on international experience, for triggering such a requirement under the *Privacy Act*. PIAs [Privacy Impact Assessments] should be conducted by independent assessors but paid for by scheme proponents, with the Privacy Commissioner setting and monitoring appropriate standards**.35

3.26 Similarly, **the LIV [Law Institute of Victoria] suggested that government agencies and organisations should be required to prepare a privacy impact assessment if they propose to apply new technologies in a way that entails collecting more information than before, sharing it more freely than before, using existing or new information for new purposes not envisaged before, or holding it longer than before. If the Privacy Impact Assessment reveals significant risks in the view of the Privacy Commissioner, further regulation could be required, whether it be a code, regulations or new legislation**. 36

3.27 The LIV continued: We suggest that Privacy Impact Assessments will introduce a process under which due consideration should be given to the privacy rights of individuals in the context of other public interests, such as national security, law enforcement and administrative efficiency. Without a predictable, structured process to assess the privacy implications of proposals that could have a broad and significant impact on the community, each new idea is likely to attract controversy and criticism until the necessary analysis has been done.

3.28 Mr Bill O'Shea from the LIV elaborated on this during the Committee's hearing in Melbourne, suggesting that there are various ways such privacy impact assessments could be done: For example, if Medibank Private or Medicare were to change the way they collect information on behalf of members we would expect that an impact

statement as to what that change would be would be provided to all members. If that were to go through parliament we would expect that impact statement to be part of the legislation, certainly either incorporated in the second reading speech or made available to the public. ...If there were other examples where legislation was not required, we would expect the peak body for the organisation that had that information to provide a privacy impact assessment for those people in the public who were dealing with it. If, for example, it involved the Insurance Council of Australia we would expect to be required to produce for the public a privacy impact assessment of whatever they were planning to do.38

3.29 Ms Irene Graham from **EFA expressed qualified support for the concept of privacy impact assessments, but cautioned that if the OPC were to conduct the assessments, funding and resourcing issues would need to be addressed**.39

3.30 The OPC acknowledged that it encouraged the use of privacy impact assessments: We have advised that [government] departments should consider a privacy impact assessment process whereby they examine any new policy proposal in the light of the impacts on a person's privacy, and that, each step along the way, they should continuously look to see what it is they are proposing to do and whether it is the best way. Things can be done in a privacy-enhancing way rather than in a privacy-intrusive way. As we often say, the biggest invasion of a person's privacy is that their identity is stolen, so we need to address some of those issues.40

3.31 **It is also noted that the OPC is developing privacy impact assessment guidelines for public sector agencies, which the OPC considers could also be applicable in the private sector**.41 The OPC also noted that 'a wider review of the *Privacy Act* could consider the question of whether the *Privacy Act* should include provisions which provide for a privacy impact assessment to be carried out in specified circumstances.'42

32 Submission 47, p. 4 cf EFA, Submission 17A, pp 7-8.

33 Submission 47, p. 4.

34 See, for example, Office of the Victorian Privacy Commissioner, Submission 33, p. 5; LIV, Submission 37, p. 5; APF, Submission 32, p. 11.

35 Submission 32, p. 11.

36 Submission 37, pp 6-7.

37 Submission 37, p. 7.

38 Committee Hansard, 22 April 2005, p. 16.

39 Committee Hansard, 22 April 2005, pp 45-46. Note also that the issue of funding and resourcing of the OPC is discussed in further detail later in this report.

40 Committee Hansard, 19 May 2005, p. 55.

41 OPC review, p. 256.

42 OPC review, p. 256.

Excerpt 2

Medicare smartcard (p. 30)

3.59 **EFA suggested that, at the very least, an independent privacy impact assessment of the smartcard should be conducted**, and that security measures should be built into the smartcard.86

86 Submission 17, p. 24.

Excerpt 3

Biometric Passports (p. 36)

3.81 **In response to the committee's questioning on to the extent to which privacy impact assessment had been, or was being, conducted in relation to the biometric passports, a representative of DFAT replied: There have been two privacy impact assessment projects conducted so far**. One was done prior to the introduction into parliament of the legislation. That was done last year. That privacy impact assessment of course included the provisions relating to the introduction of biometric technology into Australian passports. And there is currently a biometrics- or e-passports- specific privacy impact assessment being prepared.126

3.82 The representative noted that the assessment was being prepared 'internally in consultation with privacy advocates and the Privacy Commissioner'.127

3.83 Indeed, the OPC noted that it had provided advice on the passports legislation, and that this advice had been 'taken on board'.128 Further, it was noted that **the Privacy Commissioner had been funded in the recent budget 'to work with Customs and DIMIA [Department of Immigration and Multicultural and Indigenous Affairs] and DFAT on biometrics**.'129

3.84 However, EFA advised that they believed that any privacy protection afforded by the *Privacy Act* in this context was likely to be 'weak at best'. In particular, EFA was concerned that any disclosure pursuant to a determination made by the Minister under the Passports Act would be 'authorised or required by law' and therefore fall within the category of disclosure to which the *Privacy Act* does not apply.130

3.85 Some submitters were also concerned that the chip to be implanted in passports could be read remotely, and that this could actually facilitate identity theft.131 For example, Mr Roger Clarke described the passports proposal as 'naïve and dangerous', arguing that placing enormously sensitive data into an RFID tag, including biometrics will facilitate identity theft.132

125 Submission 39, p. 4.

126 Committee Hansard, 20 May 2005, p. 2.

127 Committee Hansard, 20 May 2005, p. 2.

128 Mr Timothy Pilgrim, OPC, Committee Hansard, 19 May 2005, pp 55-56.

129 Ms Karen Curtis, OPC, Committee Hansard, 19 May 2005, p. 55.

130 Submission 17, p. 29.

131 EFA, Submission 17, pp 27-28; Mr Roger Clarke, Submission 28, p. 2.

132 Submission 28, p. 2.

Excerpt 4

Census (p. 133)

5.116 However, **the committee notes that the ABS census proposal has been released for public consultation and will also be subject to a privacy impact assessment, which will also be published**.151

151 ABS, Discussion Paper: Enhancing the Population Census: Developing a Longitudinal View, ABS 2060.0, April 2005, p. 18.

Excerpt 5

Powers of the Office of the Privacy Commissioner (p. 147)

6.39 The APF submitted that the functions and powers of the Privacy Commissioner are generally adequate, but ineffective due to lack of resources. Nevertheless, **the APF recommended a number of extended or additional powers for the Privacy Commissioner, including**:

- extending the audit function to compliance by private sector organisations with the NPPs;
- the power to initiate a code of practice to deal with particular issues affecting the private sector;
- **the power to selectively require agencies and organisations to publish details of major projects or proposals with significant privacy implications**;
- **an express role in relation to privacy impact assessments**;
- the power to issue or require corrective statements; and
- a more systematic and streamlined complaints process.56

56 Submission 32, pp 23-24; pp 26-27.

Excerpt 6

A comprehensive review (pp. 151-152)

Recommendation 1

7.4 **The committee recommends that the Australian Government undertake a comprehensive review of privacy regulation**, including a review of the *Privacy Act* 1988 in its entirety, with the object of establishing a nationally consistent privacy protection regime which effectively protects the privacy of Australians.

Recommendation 2

7.5 **The committee recommends that the Australian Law Reform Commission undertake the review** proposed in recommendation 1 and present a report to Government and to Parliament.

Excerpt 7

Emerging technologies (p. 153)

7.10 The committee is particularly concerned that the *Privacy Act* is simply not keeping up with the privacy challenges posed by new and emerging technologies. While the *Privacy Act* may have been an appropriate mechanism to respond to the technologies of the 1970s and 1980s, technology has moved at a rapid pace in the past few decades, and the *Privacy Act* has not been updated accordingly. The committee considers that the introduction of other legislation to deal with the emerging technologies, such as the Spam Act 2003, is a clear demonstration of the failure of the *Privacy Act* to adequately respond to new technologies.

7.11 The committee acknowledges calls for the *Privacy Act* to remain 'technology neutral'. Indeed, the committee considers that it is desirable for the *Privacy Act* to remain as 'technology neutral' as possible. However, **the committee believes that it is possible update the *Privacy Act* in a 'technology neutral' way to reflect the technological changes that have occurred and to enable the *Privacy Act* to deal with these new technologies**.

7.12 As mentioned above, the committee proposes that the ALRC review at recommendations 1 and 2 should examine ways to improve privacy regulation to improve its capacity to respond to emerging technologies. At the same time, the committee also agrees with some of the suggestions that were put forward during this inquiry. In particular, **the committee considers that the *Privacy Act* should be amended to set out a statutory process for the conduct of privacy impact assessments in relation to new proposals which may have a significant impact on privacy. This assessment process could be a transparent and accountable way of ensuring that privacy concerns are addressed. The committee notes that privacy impact assessments are being conducted in relation to some new proposals such as biometric passports. However, the committee is concerned that these assessments are not being conducted in an open and transparent manner. The committee considers that such assessments need to involve full public consultation and should be occurring in a transparent and accountable manner**. The committee considers that the details of this statutory privacy impact assessment process could be developed by the Australian Law Reform Commission as part of the review proposed in recommendations 1 and 2.

Recommendation 5

7.13 **The committee recommends the *Privacy Act* be amended to include a statutory privacy impact assessment process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information.**

Excerpt 8

Other technologies (pp. 154-55)

7.19 The committee notes the evidence received in relation to the privacy implications of smartcard technology, and that such technology can be either privacy enhancing or privacy invasive. The area of most immediate concern to the committee is the Medicare smartcard. **The committee heard evidence of the lack of wider public consultation in relation to the privacy implications of the Medicare smartcard. Indeed, the committee is disturbed that it appears that key stakeholders were not**

consulted prior to the introductory trial of the Medicare smartcard. The committee is also concerned about the potential for function creep in the use of the Medicare smartcard.

7.20 **The committee is similarly concerned about the lack of public consultation, and indeed, the lack of publicly available information, in relation to the government's proposed national document verification service.**

7.21 **The committee also acknowledges concerns raised in submissions and evidence in relation to the privacy implications of biometric technology and the proposed biometric passports. The committee also notes the evidence of DFAT that a privacy impact assessment is being prepared in relation to the proposed biometric passports, in consultation with the OPC. However, once again, the committee is concerned that the privacy impact assessment does not appear to be being conducted in a particularly open or transparent manner.**

7.22 **The committee notes with concern the recent authorisation by the US FDA of human microchip implants. However, the committee was reassured to learn from relevant government departments that there are no similar proposals currently planned here in Australia. Nevertheless, the committee considers that this is an issue that has significant privacy implications, and that such microchip implants should be properly regulated here in Australia.**

7.23 **The committee also notes the extensive list of other technologies raised in submissions to the inquiry, including, but not limited to: RFID; spyware; location-based services; electronic messaging; and other telecommunications technology. The committee considers that the ALRC review should examine the privacy implications of these technologies, and whether appropriate regulatory measures are in place to ensure that privacy is adequately protected in relation to these technologies. Such regulatory measures should also be consistent and as technologically neutral as possible.**

Recommendation 8

7.24 The committee recommends that the review by the Australian Law Reform Commission, as proposed in recommendations 1 and 2, include consideration of the privacy implications of new and emerging technologies with a view to ensuring that these technologies are subject to appropriate privacy regulation.

Appendix 6: Australian Law Reform Commission, Extracts from Issues Paper 31 re Review of the *Privacy Act*

Context

In January 2006, the Australian Law Reform Commission was given a reference to conduct a Review of the *Privacy Act* 1988:
http://www.alrc.gov.au/inquiries/current/privacy/terms.htm

In October 2006, the Commission published 'ALRC Issues Paper 31 Review of Privacy'. This is a very substantial document, designed to elicit reponses concerning a wide range of issues. The document is at:
http://www.austlii.edu.au/au/other/alrc/publications/issues/31/
http://www.austlii.edu.au/au/other/alrc/publications/issues/31/IP31.pdf (8MB)

The Commission's policy is to not publish Submissions made to it, and consequently it cannot be established with confidence what responses were provided to it, and by whom.

The Commission's Report is not due until March 2008.

This document identifies all parts of the text that use the term 'privacy impact assessment', and provides excerpts of them. Segments of particular significance are highlighted in bold-face type.

Excerpt 1

2. Overview of Privacy Regulation in Australia

Privacy impact statements and assessments

2.111 Primary legislation and delegated legislation that affect business may require the preparation of a Regulatory Impact Statement (RIS). An RIS is a document prepared by the department, agency, statutory authority or board responsible for a regulatory proposal following consultation with affected parties, formalising some of the steps that must be taken in good policy formulation. It requires an assessment of the costs and benefits of each option, followed by a recommendation supporting the most effective and efficient option. Subject to limited exceptions,[183] the preparation of an RIS is mandatory for all reviews of existing regulation, proposed new or amended regulation and proposed treaties which will directly affect business, have a significant indirect effect on business, or restrict competition.[184]

2.112 **One issue is whether a 'privacy impact statement' should accompany any federal, state and territory government proposal to introduce legislation that impinges on privacy.**[185]

Such a statement could include a Privacy Impact Assessment and an analysis of whether the government proposal is consistent with existing federal, state and territory laws relating to the regulation of privacy.

This may include consideration of privacy matters other than the protection of personal information. See Chapter 6 for further discussion of Privacy Impact Assessments for new legislation.

[183] Australian Government Office of Regulation Review, *A Guide to Regulation—Second Edition: December 1998* (1999), B3–B4.

[184] Ibid, B2–B3.

[185] Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

Excerpt 2

6. Powers of the Office of the Privacy Commissioner

Advice on proposed enactments

6.31 **The Commissioner is to examine a proposed enactment that would require or authorise acts or practices of an agency or organisation that might, in the absence of the enactment, be an interference with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals. The Commissioner is to ensure that any adverse effects of such proposed enactment on the privacy of individuals are minimised**.[38]

6.32 **A document prepared as the result of such examination is popularly known as a 'privacy impact statement' or 'privacy impact assessment'**. As is the case with most of the powers inherent in the functions of the Commissioner established by **the *Privacy Act***, the power to examine a proposed enactment and advise on it is relatively wide. It **does not require, however, that a Minister obtain a privacy impact assessment, or that any assessment that is obtained be acted on**.[39]

6.33 **It has been suggested that privacy impact assessments should be required for all proposed Commonwealth legislation, or all proposed Commonwealth legislation carrying a high risk of infringing privacy rights created by the *Privacy Act*.**[40]

If that suggestion were adopted, **the issue arises as to whether the task should be performed by the OPC, some other public officer (currently existing or not), or a private sector individual or organisation**.

A related question is whether all privacy impact assessments should be subject to the same requirements (including as to whom should complete the task).

6.34 **The OPC Review raised the possibility that private sector organisations that develop and implement 'large scale high privacy risk' technology should be encouraged to conduct privacy impact assessments**.[41] The OPC has recently released guidelines for agencies in this regard, and the same approach could be applied to organisations.[42] The OPC Review did not go further to discuss whether organisations planning large scale high privacy risk projects should be *required* to prepare, or obtain, a privacy impact assessment, or whether privacy impact assessments are desirable or should be required other than in relation to technology. However, **the Senate Committee privacy inquiry recommended that the *Privacy Act* 'be amended to include a statutory privacy impact assessment process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information'**.[43]

> **Question 6–6:** Should the *Privacy Act* require a privacy impact assessment to be prepared for:
>
> (a) all proposed Commonwealth legislation;

(b) other proposed projects or developments of agencies; or

(c) other proposed projects or developments of organisations?

Question 6–7: If privacy impact assessments are required:

(a) who should be involved in preparing the assessments;

(b) who should be entitled to view the results of the assessments;

(c) who should bear the cost of the assessments; and

(d) what role should the Privacy Commissioner play in overseeing any requirements placed on agencies or organisations in this regard?

[37] *Privacy Act 1988* (Cth) s 27(1)(k).

[38] Ibid s 27(1)(b).

[39] Note however that the Australian Government Department of the Prime Minister and Cabinet, ***Legislation Handbook* (1999)**, [4.7(h)(vi)] **provides that, in relation to legislative matters going before Cabinet, it is expected that the relevant department undertake other consultations in preparing the submission, including 'with the Privacy Commission if the legislation has implications for the privacy of individuals'**.

[40] Office of the Privacy Commissioner and Acting NSW Privacy Commissioner, *Consultation PM 9*, Sydney, 24 July 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

[41] Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 256. This possibility was also discussed in the following consultations: Office of the Privacy Commissioner and Acting NSW Privacy Commissioner, *Consultation PM 9*, Sydney, 24 July 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

[42] See Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006).

[43] Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 5. It is not clear whether this relates to agencies and/or organisations. The OPC has defined 'project' to include any proposal, review, system, database, program, application, service or initiative that includes the handling of personal information: Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006), 3. The ALRC understands 'developments' to refer to new technological developments, such as biometrics.

Excerpt 3

6. Powers of the Office of the Privacy Commissioner
Further obligations on agencies and organisations

6.174 The OPC Review noted that a 'number of submissions put the view that at present, the *Privacy Act* does not provide sufficient powers to ensure that businesses are aware of their obligations to protect privacy, or know how to implement them in practice and carry through on implementation'.[264] Some **suggestions about further obligations on agencies and organisations made to the OPC Review, the Senate Committee privacy inquiry or the ALRC have included**:

- extending the Commissioner's audit powers to the private sector;
- introducing self-auditing and reporting requirements;
- requiring organisations to make available an approved internal dispute resolution process;[265]
- requiring organisations when collecting information to inform individuals of their ability to make a complaint about a privacy issue;[266]
- **requiring the preparation of privacy impact assessments in more situations**;[267]
- requiring mandatory reporting of privacy breaches.[268]

[264] Office of the Privacy Commissioner, Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988 (2005), 135.

[265] Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.24], [6.37].

[266] Office of the Privacy Commissioner, Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988 (2005), 160 and Rec 41. See also Ch 4.

[267] Ibid, 256; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 5; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

[268] See Question 4–35 and Question 11–3(d). See also N Miller, 'Data Leaks Under Review', *The Sydney Morning Herald* (Sydney), 8 August 2006, 27; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006 and M Crompton and R McKenzie, *Consultation PC 3*, Sydney, 24 February 2006.

Excerpt 4

7. Interaction, Fragmentation and Inconsistency in Privacy Regulation
Census and Statistics Act 1905 (Cth)

7.92 The Australian Bureau of Statistics (ABS) conducts a census of population and housing every five years in accordance with the *Census and Statistics Act 1905* (Cth).[173] The census is regarded as the most important source of statistical information in Australia. The information from the census is used to produce statistical data for use by governments, as well as academics, industry, businesses and private

individuals. The ALRC is interested in hearing whether personal information collected for the purposes of the *Census and Statistics Act* is adequately protected.

7.93 In the late 1970s, the ALRC conducted an inquiry into privacy issues and the census, culminating in the release in 1979 of *Privacy and the Census* (ALRC 12).[174] The report made a number of recommendations directed to the protection of personal information collected as part of the census.[175] A number of these recommendations have been implemented.[176]

7.94 Following the release of ALRC 12 the *Privacy Act* was enacted. The *Privacy Act* applies the IPPs to personal information collected as part of the census.[177] For example, personal information collected by the ABS for a census is likely to be regarded as collection for a lawful purpose directly related to a function or activity of the ABS and necessary and directly related to that purpose.[178] The *Census and Statistics Act* also contains a number of provisions, including secrecy provisions, directed to the protection of information collected as part of the census.[179] For example, s 19A provides that the Statistician or an ABS officer must not at any time during the period of 99 years from the day for a census divulge or be required to divulge information contained in a census form to an agency, a court or a tribunal.[180]

7.95 Before the 2001 Census, all name-identified information from past census was destroyed on completion of statistical processing. In 2000, the Australian Government introduced legislation that provided for the retention of census data.[181] This legislation was put in place for the 2001 Census on a trial basis. The *Census Information Legislation Amendment Act 2006* (Cth) amended the *Census and Statistics Act* to ensure that, subject to the household's consent, name-identified information collected in the 2006 Census and all subsequent census would be stored by the National Archives to be preserved for release for future research after a closed access period of 99 years.[182]

7.96 Another recent development is the Census Data Enhancement (CDE) project.[183] **The primary objective of the CDE project was to enhance the value of the census by combining it with future census and possibly other datasets held by the ABS. The central feature would have been the Statistical Longitudinal Census Dataset (SLCD) involving all respondents to the census**. A Discussion Paper on the project was released in April 2005[184] and a Privacy Impact Assessment (PIA) was prepared.[185] Although there was some support for the project, **a number of submissions and the PIA identified significant privacy-related concerns**.[186] In particular, the PIA noted that the proposal will create a data resource so rich and valuable for administrative uses that the privacy and secrecy framework under which the ABS operates may come under great and possible irresistible pressure, if not immediately, then at least in the medium to long term … Despite the rigour of the legislative protections, and the ABS track record both of procedural safeguards and of defence of the principle of confidentiality, there remains a residual privacy risk of future changes in legislation to allow administrative and other nonstatistical uses.[187]

7.97 On 18 August 2005, the ABS announced that it would not proceed with the SLCD as proposed and that the CDE proposal had been substantially modified.[188] **The SLCD will now be based on a 5% sample of the population**. It is the ABS's view that the reduction of the dataset to a 5% sample will make the dataset unsuitable for administrative and other non-statistical uses. Despite the modifications, the APF still have a number of concerns about the proposal, including that data collected in each census will now be retained and linked, will cover one million people, and may be used in conjunction with data from other sources.[189]

[173] Census and Statistics Act 1905 (Cth) s 8.

[174] Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979).

[175] Ibid, x–xvi.

[176] See, eg, Census Information Legislation Amendment Act 2000 (Cth).

[177] The ABS is an 'agency' for the purposes of the *Privacy Act*: *Privacy Act 1988* (Cth) s 6. For a discussion of how the IPPs apply to the census see House of Representatives Legal and Constitutional Affairs Committee—Parliament of Australia, *Saving Our Census and Preserving Our History* (1998), Ch 4.

[178] *Privacy Act 1988* (Cth) s 14, IPP 1.1.

[179] *Census and Statistics Act 1905* (Cth) ss 7, 8A, 13, 19, 19A, and 19B. Further, the *Statistics Determination 1983* (Cth) made by the Minister under *Census and Statistics Act 1905* (Cth) s 13 provides for the disclosure, with the approval in writing of the Statistician, of specified classes of information.

[180] See House of Representatives Legal and Constitutional Affairs Committee—Parliament of Australia, *Saving Our Census and Preserving Our History* (1998), Rec 1. See also Explanatory Memorandum, Census Information Legislation Amendment Bill 2006 (Cth).

[181] Census Information Legislation Amendment Act 2000 (Cth).

[182] Explanatory Memorandum, Census Information Legislation Amendment Bill 2006 (Cth).

[183] Australian Bureau of Statistics, *Census of Population and Housing—Census Data Enhancement* <www.abs.gov.au> at 25 August 2006.

[184] Australian Bureau of Statistics, Enhancing the Population Census: Developing a Longitudinal View (2005).

[185] Pacific Privacy Consulting, Census Enhancement Project: Privacy Impact Assessment Report for Australian Bureau of Statistics (2005).

[186] See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.113]–[5.116].

[187] Pacific Privacy Consulting, Census Enhancement Project: Privacy Impact Assessment Report for Australian Bureau of Statistics (2005), 3.

[188] Australian Bureau of Statistics, 'ABS Develops a New View of Records Across Successive Censuses' (Press Release, 18 August 2005).

[189] Australian Privacy Foundation, *Privacy Concerns with the 2006 Census* (2006) <www.privacy.org.au/Campaigns/Census> at 24 August 2006.

Excerpt 5

7. Interaction, Fragmentation and Inconsistency in Privacy Regulation Anti-Money Laundering and Counter-Terrorism Financing Bill 2006

7.105 On 13 July 2006, the Minister for Justice and Customs, Senator the Hon Chris Ellison, released for public consultation a revised exposure draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) (AML/CTF Bill 2006) and draft Anti-Money Laundering and Counter-Terrorism Financing Rules (AML/CTF Rules).

7.106 The AML/CTF Bill 2006 is intended to enable individual businesses to manage money laundering and terrorism financing risks. The Bill sets out the primary obligations of 'reporting entities' when providing 'designated services'. A 'reporting entity' is a financial institution, or other person who provides 'designated services'.[199] A large number of 'designated services' are listed in the Bill including opening an account, making a loan, and supplying goods by way of hire purchase.[200]

7.107 The Bill requires a reporting entity to carry out a procedure to verify a customer's identity before providing a designated service to the customer.[201] In addition, reporting entities must give the Australian Transaction Reports and Analysis Centre (AUSTRAC) reports about suspicious matters,[202] and must have and comply with an anti-money laundering and counter-terrorism financing program.[203] The Bill also imposes various record-keeping requirements on reporting entities.[204] For example, a reporting entity must make a record each time it provides a designated service and must retain the record for seven years.[205]

7.108 Part 11 of the Bill relates to secrecy and access. Except as permitted by the Bill, an AUSTRAC official, a customs officer or a police officer must not disclose information or documents obtained under the Bill.[206] Further, a reporting entity must not disclose that it has reported, or is required to report, information to AUSTRAC; or that it has formed a suspicion about a transaction or matter. The Part also provides that the Australian Taxation Office and certain other 'designated agencies' may access AUSTRAC information. The term 'designated agencies' is defined in cl 5 to include a large number of Australian Government agencies as well as some state and territory agencies. Designated agencies may access AUSTRAC information for the purposes of performing that agency's functions and exercising the agency's powers.[207] The Bill requires designated agencies, including state and territory agencies, to comply with the IPPs in respect of the accessed AUSTRAC information.[208]

7.109 The revised exposure draft AML/CTF Bill 2006 and draft AML/CTF Rules reflect consideration of over 120 submissions provided to the Attorney-General's Department following the release of the first exposure Bill on 16 December 2005,[209] and **the findings of the Senate Legal and Constitutional Legislation Committee inquiry into the exposure draft Bill**.[210] **The Committee concluded that an independent privacy impact assessment of the Bill should be conducted**. The Committee also recommended that the Bill should contain a statement that is reflective of the intention to allow federal, state and territory agencies to access and utilise AUSTRAC data for purposes that may not be related to anti-money laundering or counter-terrorism financing.[211] These recommendations have not been included in the latest revised exposure draft of the Bill.

7.110 Submissions in response to the revised exposure draft AML/CTF Bill 2006 continue to raise privacy issues. For example, the OPC and the APF have both observed that while Part 11 of the Bill imposes some privacy obligations on state and territory agencies accessing AUSTRAC information, not all states and territories have enacted privacy regimes. Therefore, it is unclear whether individuals will be able to make complaints and seek remedies if information has been dealt with inappropriately by these agencies.[212]

7.111 Submissions have also noted that the NPPs may not provide adequate protection of personal information collected and disclosed under the Bill. For example, reporting entities that are 'organisations' for the purposes of the *Privacy Act* will have to comply with the NPPs. However, the NPPs will generally not apply to reporting entities that are small businesses.[213] A proportion of the reporting entities that are collecting and sharing personal information for the purposes of the Bill therefore may not be subject to any privacy regulation.

7.112 Under Part 10 of the Bill a reporting entity must retain for seven years information contained in a suspicious matter report to AUSTRAC. However, the Bill prevents an individual from seeking access to that information under NPP 6. The OPC has therefore suggested that, as an individual is not able to check information that is held about his or her, and has no opportunity to provide clarifying details or correct errors, further limitations on the retention of information by reporting entities are warranted.[214] It has also been observed that cl 110 of the Bill makes it an offence to provide a designated service on an anonymous basis. This directly contradicts NPP 8 which provides that wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.[215]

7.113 The Attorney-General's Department is currently reviewing the submissions received during the second consultation period and is finalising the legislative package for introduction to Parliament later in 2006. The ALRC is interested in views on how the Bill interacts with the *Privacy Act* and whether the Bill adequately protects personal information.

[199] Revised Exposure Draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) cl 5.

[200] Ibid cl 6.

[201] Ibid pt 2.

[202] Ibid pt 3.

[203] An anti-money laundering and counter-terrorism financing program is a program that is designed to identify, mitigate and manage the risk a reporting entity may face when providing designated services in Australia that might involve or facilitate money laundering or financing of terrorism: Ibid cl 74.

[204] Ibid pt 10.

[205] Ibid cl 85.

[206] See, eg, Ibid cl 93.

[207] Ibid cl 99.

[208] Ibid cl 99(3).

[209] See Australian Government Attorney-General's Department, *Welcome to Anti-money Laundering Reform Online* <www.ag.gov.au> at 27 August 2006.

[210] Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005* (2006).

[211] Ibid, [4.72]–[4.76].

[212] See, eg, Australian Government Office of the Privacy Commissioner, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, 3; Australian Privacy Foundation, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, August 2006, 57.

[213] See, eg, Australian Government Office of the Privacy Commissioner, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, 3–4; Australian

Privacy Foundation, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, August 2006, 62; Chartered Secretaries Australia, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, August 2006.

[214] Australian Government Office of the Privacy Commissioner, Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006, 4.

[215] Ibid, 5.

Excerpt 6

11. Developing Technology

11.37 In 2006, **the Australian Government released part of a framework to assist agencies seeking to implement smart card technology**.[65] **The framework requires** agencies implementing smart card technologies to include data protection clauses in agreements with third parties about the supply of smart cards and related services, and **privacy impact assessments to be undertaken during the design of smart card systems**. It also requires agencies implementing smart card technologies to produce comprehensive privacy policy statements and to revise these statements 'whenever a third party agency adds additional functionality to an existing smartcard deployment'.[66]

[65] Australian Government Information Management Office, *Australian Government Smartcard Framework* (2006).

[66] Ibid, [a.17].

Excerpt 7

11. Developing Technology

11.47 On 27 July 2006, the Privacy Commissioner announced the approval of the *Biometrics Institute Privacy Code*.[95] The preamble to the Code notes that 'Biometrics Institute members understand that only by adopting and promoting ethical practices, openness and transparency can these technologies gain widespread acceptance'.[96] The Code is binding on Biometrics Institute members who sign the Biometrics Institute Privacy Code Agreement to Comply.[97] To date, two organisations have agreed to be bound by the Code.[98]

11.48 The Code aims to: (i) facilitate the protection of personal information provided by, or held in relation to, biometric systems; (ii) facilitate the process of identity authentication in a manner consistent with the *Privacy Act* and the National Privacy Principles (NPPs); and (iii) promote biometrics as PETs.[99] It includes information privacy standards that are at least equivalent to the NPPs.[100] In addition, it requires organisations that have agreed to be bound by the Code to observe higher levels of privacy protection than those in the NPPs in certain circumstances. For example, the Code applies to acts and practices relating to employee records that are exempt from the operation of the *Privacy Act* if a biometric is included as part of the employee record, or has a function related to the collection and storage of, access to, or transmission of an employee record.[101]

11.49 **The [Biometrics] Code** also contains three new information privacy principles. Principle 11 (Protection) sets out the steps that Code subscribers must take to protect biometric information, including ensuring that biometric information is de-identified where practicable, only stored in encrypted form and is not held in a way that makes it easy to match to other personal information. Principle 12 (Control) requires enrolment in biometric systems to be voluntary, and prevents organisations from using biometric information for some secondary purposes without 'free and informed consent'. **Principle 13** (Accountability) requires individuals to be informed of the purposes for which a biometric system is being deployed. It also requires biometric systems to be audited and Code subscribers to adopt a holistic approach to privacy policy and procedures. In addition, it **mandates the use of privacy impact assessments as part of the planning and management process for biometrics implementation**.

[Note: virtually no organisations at all have subscribed to the Biometrics Code, and it does not even automatically apply to members of the organisation that sponsored it]

[95] K Curtis (Privacy Commissioner), 'Privacy Commissioner Approves Biometrics Institute Privacy Code' (Press Release, 27 July 2006).

[96] Biometrics Institute, *Biometrics Institute Privacy Code* (2006), Preamble, [2].

[97] Ibid, [C.1], [C.2].

[98] Biometrics Institute, Biometrics Institute Privacy Code—Public Register (2006) <www.biometricsinstitute.org> at 4 September 2006.

[99] Biometrics Institute, *Biometrics Institute Privacy Code* (2006), [B.1].

[100] K Curtis (Privacy Commissioner), 'Privacy Commissioner Approves Biometrics Institute Privacy Code' (Press Release, 27 July 2006).

[101] Biometrics Institute, *Biometrics Institute Privacy Code* (2006), [D.5].

II. New South Wales

N.S.W. is a State of about 800,000 square kilometers (20% larger than France). It has a population approaching 7 million, almost 75% of whom live in the Newcastle-Sydney-Wollongong conurbation.

Legislative and Policy Framework

Legislation

From 1975 until 1999, the NSW Privacy Committee operated as a research and complaints-handling body. Since 1999, there has been an Office of the New South Wales Privacy Commissioner (Privacy NSW).[32] The Commissioner on a part-time basis from 1999 until May 2003 was Chris Puplick. Since September 2003, John Dickie, sometime Chief Censor, has been Acting in the position, full-time since the end of 2004, but on rolling short-term contracts.

The primary legislation is the *Privacy and Personal Information Protection Act* (PPIPA).[33]

Relevant New South Wales laws include:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *Freedom of Information Act 1989*
- *State Records Act 1998*
- *Criminal Records Act 1991 (Spent Convictions)*
- *Listening Devices Act 1984*
- *Workplace Surveillance Act 2005*
- *Telecommunications (Interception and Access) (New South Wales) Act 1987*
- *Access to Neighbouring Land Act 2000, esp. s.16 and s.26.*
- *Crimes (Forensic Procedures) ACT 2000*[34]

PIA Guidance Material

There is currently no official PIA guidance material in NSW. The web-page for Government, which appears to have been in its present form since about 2004, refers to PIAs as follows:

"PIA involves a comprehensive analysis of the likely impacts of a project upon the privacy rights of individuals. It is a little ... like an environmental impact assessment done for a new development proposal. The assessment can ensure that any problems are identified – and resolved – at the design stage. PIA is not only about ensuring compliance with the relevant information privacy laws (such as the PPIP Act and the HRIP Act), but can also help to minimise the risk of reputational damage by identifying broader privacy concerns (such as bodily or territorial privacy impacts).

[32] The NSW Privacy website is at: http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_index.
[33] The Act may be found at: http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/.
[34] Listed on the Privacy Commissioner of Australia website at: http://www.privacy.gov.au/privacy_rights/laws/ and Australian Privacy Foundation website at: http://www.privacy.org.au/Resources/PLawsST.html#NSW.

"**Privacy NSW hopes to develop a guide to conducting PIAs in the near future**. Similar jurisdictions to NSW have or are currently developing their own guides; if you would like to find out more about these please contact Privacy NSW".[35]

The page offers a checklist of privacy issues that agencies may need to address. The hotlink is broken, but it can be found at:

https://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/privacyessentials_03_2005.pdf/$file/privacyessentials_03_2005.pdf

The following extract is taken from the Commission's June 2004 Submission to a Review of the Privacy and *Personal Information Protection Act 1998*. It cited Blair Stewart's papers, and referred to the literature and brief history in one of this author's papers (emphasis added).

> "Under the PPIP Act, public sector agencies are required to prepare and publish Privacy Management Plans in relation to their compliance with the Act. However Privacy Management Plans do not embrace matters outside the regulatory scope of the PPIP Act, nor do they relate to specific projects, and there is no requirement to update their plans as new initiatives are being considered. **Our success in getting agencies to measure privacy impacts before undertaking new practices or projects has mostly been limited to ensuring compliance with regulatory requirements.**
>
> "**By contrast, a Privacy Impact Assessment (PIA) is a process whereby a conscious and systematic effort is made to assess the privacy impacts of options that may be open in regard to a proposal. PIA is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated**.
>
> "A well-conducted PIA can provide assistance not only in terms of compliance with relevant privacy law, but also guidance for measuring the privacy impact of projects and practices which are not governed by information privacy laws. PIAs would also heighten the awareness and importance of privacy generally, and will bolster efforts to make privacy consideration part of the 'mainstream' legal and policy landscape.
>
> "Privacy Impact Assessment has been mentioned in the privacy literature from the 1980s, and implemented in jurisdictions from the early 1990s. PIAs have often been promoted by Privacy Commissioners as a way of encouraging more self-reliance by agencies, in terms of building expertise in privacy assessment outside of just the Commissioner's office.
>
> "Privacy and data protection commissioners have a central role in respect of the protection of privacy. However, they invariably have small budgets and few staff. It is absurd to expect that Commissioners can assess all the various technological initiatives likely to impact upon citizens' privacy in the coming years. The responsibility must be shared.
>
> "**The objectives of a PIA** may be to:
>
> - **assess risks arising from a new technology** or the convergence of existing technologies (for instance, electronic road pricing, caller ID, smart cards);
> - **assess risks where a known privacy intrusive technology is to be used in new circumstances** (for instance, expanding data matching or drug testing, installation of video surveillance cameras in further public places);
> - **assess risks in a major endeavour or change in practice having significant privacy effects** (for instance, a proposal to merge major public registries into a "super registry", to adopt a national ID card, to relax controls on telephone tapping or to extend powers of search of premises or persons); and to develop strategies for minimising those risks.

[35] http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_forgovt.

> "**PIAs, if published, can also address reputational risk areas for government, and can assist other similar projects by providing a ready-made analysis of likely risk areas and possible solutions**.
>
> "In the last few years PIAs have become compulsory for large federal government projects in the United States and Canada, and they have also been undertaken voluntarily by agencies in Hong Kong and New Zealand. A recent example from New Zealand, published on the Privacy Commissioner's website, related to the State Services Commission's project on authentication for e-government purposes.
>
> "In 2002 **the New Zealand** Privacy Commissioner published a **Privacy Impact Assessment Handbook** which provides guidance to both public and private organisations about how to conduct PIAs. The Handbook **is an exemplar of guidance and leadership in the area of best privacy practice**.
>
> "We understand that both the Office of the Federal Privacy Commissioner and the Victorian Privacy Commissioner are currently working on their own PIA handbooks, as they each recognise the growing importance of PIA as a valuable assessment tool for governments when developing new legislative and technological projects and policies.
>
> "**We believe that PIAs are the best means by which government agencies can aim for best privacy practice as well as legislative compliance. It is our submission that ideally, a PIA would be a statutory requirement for any new Bill, regulation, or project significant enough to require Cabinet consideration**.
>
> "One possible model would be:
>
> - Privacy NSW to help set terms of reference for a PIA, including what external guidelines / standards to use
> - PIA to be conducted by an independent consultant, who reports to Privacy NSW as well as the client
> - final PIA report to be published" [36]

The Commission has been starved of resources since mid-2004, and there appears to have been no subsequent progress.

On the other hand, the following extracts from the Privacy Commission's February 2007 Submission to the Australian Law Reform Commission's Review of federal Privacy Law indicates that it continues to be supportive of the notion, at least at federal level:

> "**Privacy legislation should make it mandatory for all Commonwealth agencies and private organisations to provide and publish Privacy Impact Assessments (PIAs) for all new programs, policies and draft legislation which impacts on the handling of 'personal information'. The PIA provides for accountability and greater transparency in decision-making.**
>
> "If PIAs were mandatory in certain circumstances, **it would create a consistent framework for the early identification of actual or potential privacy risks during the design and/or redesign of legislation, programs and services**. For example, the early identification of privacy risks in major IT projects has the potential to prevent costs that may be incurred through rushed modifications if the risk is identified late in the development process. In addition, the requirement for PIAs would create more awareness of the importance of privacy and make privacy compliance a fixture in today's legal and policy landscape.
>
> "Formalisation of the role of the Privacy Commissioner in regard to consultation of this nature concerning initiatives that impact on information privacy would only serve to have

36

http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/sub_ppipareview.pdf/$file/sub_ppipareview.pdf#target='_blank'.

a positive effect on privacy protection. A PIA can provide assistance with compliance as well as a barometer for measuring the privacy impact of projects and practices.

"**The Privacy Commissioner could provide a guideline or 'template' for PIAs**, as well as input into matters which the OPC feels should be addressed with a specific assessment for comprehensiveness of outcome. However, we envision that **either an external consultant or the Privacy Commissioner could undertake a PIA**, provided there are no conflicts of interest.

"**The financial cost for PIAs should be shouldered by the agency/organisation seeking to initiate the new/revised legislation, program or services**. This prerequisite would be on the same order or similar to the requirement of environmental impact statements prior to proposed undertakings in the mining or construction industries. **To ensure openness and accountability, copies of these assessments should be provided to the Privacy Commissioner and made available to the public**".[37]

Completion of PIAs

Privacy NSW is aware that a few agencies have conducted PIAs. Although mention has been made in various discussions of PIAs in the health and education spheres, no evidence was found.

If anything, the tendency is in the other direction: the Government has suspended a Health Privacy Principle in respect of a major pilot project in the health care arena, because the pilot would otherwise have been in breach of the Act.[38]

[37] at http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/sub_alrc2007.pdf.
[38] http://www.smh.com.au/news/national/no-privacy-guarantee-on-new-health-records/2006/04/04/1143916530284.html http://www.smh.com.au/news/national/reversal-of-privacy-promise/2006/02/24/1140670269206.html. See also http://www.privacy.org.au/Campaigns/E_Health_Record/HealthElink.html.

III. VICTORIA

Victoria is a State of about 230,000 square kilometres (about the same as the U.K.). It has a population of 5 million, 75% of whom live in the capital city.

Legislative and Policy Framework

Legislation

A conventional statute, the *Information Privacy Act 2000*, came into effect in late 2002.[39]

There is also a separate Health Records Act.[40]

The *Information Privacy Act* created the statutory post of Privacy Commissioner. The post is supported by the Office of the Victorian Privacy Commissioner (OVPC), or Privacy Victoria.[41]

Relevant Victoria laws include:

- *Charter of Human Rights and Responsibilities Act 2006 (which includes reference to privacy)*
- *Information Privacy Act 2000*
- *Health Records Act 2001*
- *Freedom of Information Act 1982*
- *Public Records Act 1973*
- *Surveillance Devices Act 1999*
- *Telecommunications (Interception) (State Provisions) Act 1988* [42]

PIA Guidelines

In August 2004, the Commissioner published a 'Privacy Impact Assessment Guide'.[43]

The Australian Privacy Foundation expressed reservations, including: "the document may be a guide for Privacy Law Compliance Audit, but not for Privacy Impact Assessment. In addition, the document makes repeated mentions of the IPPs and the Information Privacy Act, and does not refer to the many additional laws that establish privacy protections" [and] "most of the Guide is written as though the exercise was purely internal".[44]

The Commissioner has communicated the existence of the PIA Guidelines through its network of privacy officers in government agencies, conducted a training session, and mentioned the PIA Guidelines in various presentations.

---

[39] http://www.austlii.edu.au/au/legis/vic/consol%5fact/ipa2000231/index.html
[40] http://www.austlii.edu.au/au/legis/vic/consol%5fact/hra2001144/index.html
[41] http://www.privacy.vic.gov.au/
[42] Office of the Privacy Commissioner of Australia at: http://www.privacy.gov.au/privacy_rights/laws/#2 and Australian Privacy Foundation, http://www.privacy.org.au/Resources/PLawsST.html#Vic.
[43] At: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf.
[44] http://www.privacy.org.au/Papers/OFPC-PIA-0502.rtf.

It is understood that the Department of Justice used the Commissioner's Guide as a basis for a practical document suitable for practitioners in the Department's organisational sub-units.

A draft document, presumably of 2005-06, implies that the Victorian Government Identity Management Framework suggests that a PIA be undertaken as part of projects that involve identity authentication[45]; but no final document could be found.

The Victorian PIA Guidelines

The PIA Guide of August 2004 references prior work, particularly in New Zealand, Canada and Hong Kong, and at federal level in Australia.

Key features include the following:

- it is specifically addressed to government agencies;
- it uses Blair Stewart's description of a PIA as "a systematic process for identifying and addressing privacy issues";
- it is limited throughout to the scope of the Victorian Act, and in particular to compliance with the legal requirements expressed primarily in the Information Privacy Principles;
- agencies are subject to no obligations in relation to PIAs. The Guide states, however that "A PIA should be completed for any new project or system, or any significant revision or extension of an existing system, involving the collection and handling of personal information" (p. 3, emphasis added in this document);
- "Ideally, a PIA should be initiated at the early stages of project or system development and planning" (p. 3);
- "Often, a PIA will be useful more than once in the project's life" (p. 3);
- "the object of a PIA is not to 'sell' an idea that may have adverse privacy implications. The primary object of a PIA is to allow any adverse effect on privacy to be weighed properly against whatever benefits the project or system offers in the public interest" (p. 4);
- "A [PIA] can be performed by: "an individual from within the organisation; a team or section from within the organisation; a joint team or working group if more than one organisation is involved in a project; or an external body ... [but] it will still be important for the organisation to have overall responsibility for the PIA" (p. 9);
- "PIAs form part of the risk evaluation and management tasks for any substantial undertaking" (p. 11);
- although the document mentions "public consultation as part of a PIA" and "publishing a PIA once it is complete", it expresses neither requirements nor recommendations (p. 13);
- in the case of agencies exempted from the Act ,or business processes that may be the subject of exceptions within the Act, it appears to absolve the agency of any responsibility to conduct a PIA (p. 14).

45 http://www.dtf.vic.gov.au/CA25713E0002EF43/WebObj/IDAInternalGuidelinesOverview/$File/IDA%20Internal%20Guidelines%20Overview.pdf

Review of the Guidelines

The Commissioner has stated her intention to review the Guidelines in the near future, with the expectation that key messages will be strengthened and clarified. Some of the elements of this may include:

- the agency's responsibility to perform PIAs where privacy impacts of a measure may be significant;
- the benefits of using specialist support, at least in relation to the framing and planning of the PIA, even if the assessment itself is undertaken by agency staff;
- the Commissioner's role in PIAs, which she sees as being as a stakeholder, as an advisor prior to the commencement of the assessment, and as a discussant and reviewer of the outcomes, but not as a formal 'approver' of PIA processes or reports;
- the benefits of involving the affected public, their representatives, and advocates for their interests. These include deeper understanding of the impacts, and ways of solving the problems;
- the benefits of publishing the existence of PIA processes;
- the benefits of publishing the resulting PIA report;
- appropriate ways to deal with the media in relation to PIAs, in order to avoid trivialisation and mis-reporting, but nonetheless achieve a suitable level of transparency.

Practical advice to practitioners on how to go about doing a PIA is important, because agencies have conveyed the message that without it they are reluctant to adopt the technique.

Completion of PIAs

Examples of PIAs Conducted

It is understood that a small number of PIAs have been performed in Victoria, including one on a pilot health smartcard scheme.

The only published document of the nature of a PIA that could be located was performed by the Department of Education & Training (DET). It related to an R&D initiative, undertaken jointly with Oracle, to produce a prototype student-centric information system known as Ultranet. One feature of the scheme is a unique student identifier intended for all Victorian students, at all levels.[46]

The document is limited to a Privacy Act Compliance check, and involved little or no consultation with affected parties. It is understood that the Department intends to conduct a full PIA, but has not yet done so even in respect of the identifier, far less in relation to the project as a whole.

The Commissioner is aware of many agencies claiming to have conducted PIAs, but only a small number have involved consultation with her Office. Many of those that have come to her notice have been quite limited in their scope, and agencies appear to have been reluctant to expose them.

[46] The document is an undated draft apparently of June 2006, at: http://www.eduweb.vic.gov.au/edulibrary/public/teachlearn/student/S@CPIAReport.doc.

The Commissioner is not aware of any PIA Reports having been published, and indeed is not aware of any public declarations by agencies of PIAs being conducted, or having been conducted.

External Consultation

The Guidelines mention public consultation as part of a PIA, but express neither requirements nor recommendations.

Public Availability

The Guidelines mention the publication of a PIA once it is complete, but express neither requirements nor recommendations

IV. QUEENSLAND

Queensland is a State of about 1.8 million sq.km. (Spain, France, Germany and Poland combined), ranging from lush coastal lands via rich agricultural country to semi-desert. It has a population of 4 million, of whom about 55% live in the Brisbane-Ipswich-Gold Coast conurbation.

Legislative and Policy Framework

Legislation

There is no privacy legislation, and no statutory privacy protection body in Queensland. A regulatory framework exists in the form of an unenforceable code expressed in two Government Standards – No. 42, plus No. 42A for health matters.[47] The Standards reflect the federal National Privacy Principles. They apply to almost all government agencies, but not to local government:

The Privacy Standard requires production of 'Privacy Plans', which detail how each agency has implemented the Principles.[48]

Relevant Queensland privacy laws include:

- *Freedom of Information Act 1992*
- *Public Records Act 2002*
- *Criminal Law (Rehabilitation of Offenders) Act 1986* (spent convictions)
- *Invasion of Privacy Act 1971*(listening devices, invasion of privacy of the home)
- *Whistleblowers Protection Act (1994)*
- *Police Powers and Responsibilities Act 2000* (Chapter 4 deals with Covert Evidence Gathering Powers) [49]:
- No state telecommunications interception power
- *Grosse v Purvis [2003] QDC 151 (16 June 2003)*
- *Private Employment Agents (Code of Conduct) Regulation 2005* (Provisions 14 and 15 deal with work seekers information and the need to ensure it is not disclosed or improperly used)

A small Privacy Unit within the Department of Justice and Attorney-General has some some responsibilities relating to privacy. The Department uses the label 'Queensland

[47] Current Information Standards, Guidelines and Reviews, IS42 and IS42A, Queensland Government at: http://www.governmentict.qld.gov.au/02_infostand/standards.htm.
[48] Futher explained at: http://www.privacy.qld.gov.au/plan.htm.
[49] From: http://www.privacy.gov.au/privacy_rights/laws/#3. This list and further notes are available at the Australian Privacy Foundation webpage at: http://www.privacy.org.au/Resources/PLawsST.html#Qld.

Privacy' for the web-page, but whereas in NSW and Victoria that form of title indicates a government agency, in this case it appears to be a slogan or brandname.[50]

Guidance Relating to PIAs

The Department of Justice and Attorney-General) has been conducting preliminary work and promising PIA guidance material since 2005.

Issue 2 of a newsletter called *Queensland Privacy (in focus)* in December 2005, stated that:

> "Privacy Impact Assessment (PIA) Annotated Questionnaire has been piloted in some Queensland Government agencies in relation to proposed programs and initiatives. Work continues on the questionnaire in relation to expanding use of the PIA process to assess proposed legislation or legislative amendments.
>
> "PIA guidelines will be available in February 2006 as a decision-making and privacy assessment tool complimentary [sic] to the PIA annotated questionnaire".[51]

Issue 3 in March 2006 stated that:

> "Privacy Impact Assessment (PIA) Annotated Questionnaire and Instructions—A 2-part PIA Annotated Questionnaire (1— Proposed programs, 2—Proposed legislation) and the complimentary [sic] completion instructions are in the final drafting stage and will be made available online shortly".[52]

Issue 6 in December 2006 stated that:

> "Privacy Impact Assessment (PIA) annotated questionnaire and instructions available online soon".[53]

At this stage, however, only the following guidance is provided:

> "What is a PIA?
>
> "**A Privacy Impact Assessment (PIA) is a due diligence exercise, allowing Queensland Government agencies (including relevant contractors, vendors, outsourcers and others) to identify and address potential privacy risks** that may occur during the course of their operations.
>
> "PIAs provide a thorough **description and analysis of a program, potential privacy risks** associated with the program, **and measures taken to minimise or eliminate such risks**. The PIA process may also be used to examine proposed legislation or legislative amendments.
>
> "When should Queensland government agencies conduct a PIA?
>
> "PIAs should be conducted whenever a program involving the collection, storage, use and/ or disclosure of personal information is proposed, or where existing programs may be substantially changed. PIAs should also be conducted where legislation (or a legislative amendment) affecting personal information is proposed.

[50] See http://www.privacy.qld.gov.au/ for the privacy guidance material provided by this agency and http://www.justice.qld.gov.au/dept/privacy.htm for information about the privacy scheme.
[51] At: http://www.privacy.qld.gov.au/publications/INfocus2.pdf.
[52] At: http://www.privacy.qld.gov.au/publications/INfocus3.pdf.
[53] at: http://www.privacy.qld.gov.au/publications/INfocus6.pdf.

> "It is not mandatory for Queensland government agencies to conduct PIAs, however **completed PIAs provide a high level of documented assurance to stakeholders (such as other Government agencies and members of the community)** that privacy issues relating to proposed programs, legislation or legislative amendments have been identified, considered and appropriately addressed.
>
> "PIA framework and agency checklist
>
> "Coming soon!
>
> "**A framework for PIAs is being developed** by the Department of Justice and Attorney-General. It will include agency checklists for proposed programs and legislation/ legislative amendments, as well as instructions for completing the checklists". [54]

Examples of PIAs Conducted

It is understood that a PIA was performed for the Department of Transport in relation to the proposed smartcard-based driver's licence, but it appears not to have been published.

No evidence was found of any other Queensland government agency having performed a PIA on any project or initiative.

[54] At: http://www.privacy.qld.gov.au/publications.htm#4.

V. WESTERN AUSTRALIA

Western Australia is a State of about 3 million sq.km. (and is the second-largest sub-national entity in the world, the size of 2/3rds of Russia west of the Urals, or close to Spain, France, Germany and the whole of Scandinavia combined). Most of it is desert or semi-desert. It has a population of about 2 million, about 75% of whom live in the capital city.

Legislative and Privacy Framework

Legislation

There is no privacy legislation in Western Australia. Relevant laws are at:

- *Freedom of Information Act 1992*
- *State Records Act 2000*
- *Spent Convictions Act 1988*
- *Surveillance Devices Act 1998*
- *Telecommunications (Interception) Western Australia Act 1996*[55]

Following the release of a Discussion Paper in 2003, the Attorney-General tabled an Information Privacy Bill in March 2007, but it has not progressed yet.[56]

The Bill contains a set of Information Privacy Principles and a separate set of Health Privacy Principles. It would expand the functions of the present Information Commissioner to that of a Privacy and Information Commissioner. Provision is made for a Deputy Commissioner, but there is no obligation to appoint one.

The Office of the Information Commissioner, which has existed since 1993, has been occupied on an Acting basis, on rolling contracts, since 2003. The Office has a total of 10 staff.[57]

The Bill would enable the post of Privacy and Information Commissioner to be held concurrently with that of Parliamentary Commissioner (Ombudsman). The Office of the Parliamentary Commissioner, which has existed since 1971.[58] The Bill contains no provisions relating to PIAs.

It does not appear that any agency is playing any interim role in relation to privacy protection.

[55] http://www.privacy.gov.au/privacy_rights/laws/#4 and http://www.privacy.org.au/Resources/PLawsST.html#WA.
[56] http://www.austlii.edu.au/au/legis/wa/bill/ipb2007241/
[57] Further information on the Office is available at: http://www.foi.wa.gov.au/.
[58] http://www.ombudsman.wa.gov.au/.

Completion of PIAs

Evidence was found of a single PIA Report. This was conducted in early 2007 in relation to a project to establish a Whole of Western Australian Government Number (WAGN) for public service employees[59].

As at 27 July 2007, the WAGN page contained the following text (emphasis added): [60]

> "**A PIA is an assessment tool that describes the personal information flows in an initiative** such as the WAGN, and analyses the possible impacts that those flows may have on the privacy of individuals. **The purpose of a PIA is to identify and recommend options for managing, minimising or eradicating privacy impacts**.
>
> "Some of the benefits of a PIA include the following:
>
> - gaining and maintaining **stakeholder acceptance** (including agencies and employees)
> - **early identification of privacy issues and risks** for the use of the WAGN by WA state government agencies
> - identifying privacy issues and risks in the disclosure or use of WAGN related information by WA state government agencies
> - **incorporating the management of identified issues and risk mitigation strategies into design** for development of the WAGN
>
> "The recommendations of the PIA will be used to inform policy, procedures and guidelines around the use of the WAGN. As **consultation with stakeholders is an important component of the PIA process**, the Office of e-Government is currently engaging with a number of WA state government agencies".

The PIA was undertaken following recommendations contained in a September 2005 consultancy report, at Appendix H (pp. 86-94).[61]

[59] http://www.egov.wa.gov.au/documents/FINALWAGNPIA.pdf
[60] "Western Australian Government Number Privacy Impact Assessment Consultation ," Office of e-Government, at: http://www.egov.wa.gov.au/index.cfm?event=consultation.
[61] "Identity and Access Management Framework," Department of the Premier and Cabinet, Western Australia Office of e-Government, September 15, 2005, http://www.egov.wa.gov.au/documents/idam_framework_final.swf.

VI. SOUTH AUSTRALIA

South Australia is a State of about 1 million sq.km. (France, Germany, Belgium and The Netherlands combined), most of it arid or semi-arid. It has a population of 1.5 million, over 70% of whom live in the capital city.

Legislative and Policy Framework

Legislation

Relevant South Australian laws include:

- *Freedom of Information Act 1991*
- *State Records Act 1997*
- *Listening and Surveillance Devices Act 1972*
- *Telecommunications (Interception) Act 1988*
- No spent convictions law, but see discussion paper (released 5 May 2004)[xvi][62]

There is no privacy legislation, and no statutory privacy protection body. A Privacy Committee of South Australia exists under proclamation of Government. It is run out of the State Records Office, and has no budget.[63]

A Handbook for Committee Members exists, which contains information on the role of the Committee, members' responsibilities and Committee processes and activities.[64]

One of the Committee's powers is to "exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Committee thinks fit" (s.4 of the Proclamation establishing the Privacy Committee). It also handles complaints, advises Government and other bodies on privacy protection measures, and watches developments elsewhere.

A Cabinet Administrative Instruction 1/89 establishes a set of Information Privacy Principles, and includes the following Clauses:

4. The principal officer of each agency shall ensure that the following Principles are implemented, maintained and observed for and in respect of all personal information for which his or her agency is responsible.

6. An agency shall not do an act or engage in a practice that is in breach of or is a contravention of the Principles. [65]

Although, as a Cabinet Instruction, it is binding on all South Australian Public Sector agencies, it is unclear by what means and by whom it could be enforced.

The Department of Health Code of Fair Information Practice (July 2004) provides guidance in relation to the handling of personal information within "the Department,

[62] at: http://www.privacy.gov.au/privacy_rights/laws/#5 and http://www.privacy.org.au/Resources/PLawsST.html#SA.
[63] "Privacy Committee of South Australia, http://www.archives.sa.gov.au/privacy/committee.html.
[64] http://www.archives.sa.gov.au/files/privacy_privacy_committee_members_handbook.pdf.
[65] The Administrative Instruction is available at: http://www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf and: http://www.archives.sa.gov.au/privacy/principles.html.

funded services providers and others who have access to Departmental personal information".[66]

The Code is derived from the National Privacy Principles, and it appears that it embodies unspecified reductions in the protections declared in the Cabinet Instruction. As with the Cabinet Instruction itself, it is unclear whether, how and by whom it could be enforced, particularly in relation to organisations that are not State government agencies and individuals who are not State government employees.

The Department of Families and Communities has a Code of Fair Information Practice, which appears to be identical to the Health Code with the exception of the substitution of Departmental name.[67]

Guidance in Relation to PIAs

Apart from mention in an Annual Report of attendance by a representative of the Committee at a PIA Seminar in Wellington N.Z. in March 2006, the Committee's documents appear not to refer to privacy impact assessment.

The Executive Officer of the Committee advised that the South Australian Government does not have a centralised programme for Privacy Impact Assessment. However, "the Privacy Committee, supported by State Records, does use a rudimentary questionnaire for programmes that require Privacy Committee approval, exemption from the Information Privacy Principles, or require consideration of complex personal information handling issues. It is a working document that is adapted to suit the situation at hand. It may be formalised later, and adopt components from other jurisdictions' structured PIAs".

The Health Code makes reference to a PIA methodology tool. The Executive Officer of the Committee advised that the Department of Health has mandated PIAs for use in the early planning stages of projects involving personal information. A copy of the PIA Guidelines and Proforma were provided. The PIA Guidelines are broader than information privacy alone, but the PIA Proforma is limited to the Information Privacy Principles.

The Department of Families and Communities Code also makes reference to a PIA methodology tool, but it is unclear whether one has been developed, and if so whether any use has been made of it.

Examples of PIAs Conducted

It is to be presumed that PIAs have been performed within the Department of Health, but no information about them appears to be publicly available.

No evidence was found of any other S.A. government agency having performed a PIA on any project or initiative.

No copies of published PIA Reports were located.

---

[66] at: http://www.health.sa.gov.au/DesktopModules/SSSA_Documents/LinkClick.aspx?tabid=57&mid=403&table=SSSA_Documents&field=ItemID&id=45&link=H%3a%5cTemp%5cHealth-Code-July04.pdf and also available from: http://www.health.sa.gov.au (under Publications / Guidelines).

[67] at: http://www.familiesandcommunities.sa.gov.au/DesktopModules/SAHT_DNN2_Documents/DownloadFile.aspx?url_getfileid=65 and is available from: http://www.familiesandcommunities.sa.gov.au (under Publications / Policies).

VII. TASMANIA

Tasmania is an island State of about 90,000 sq.km. (the same as Portugal, and twice the size of Switzerland). It has a population of close to 0.5 million, about 40% of whom live in the capital city.

Legislative and Policy Framework

Legislation

Relevant Tasmanian laws include:

- *Personal Information Protection Act 2004*
- *Freedom of Information Act 1991*
- *Archives Act 1983*
- *Annulled Convictions Act 2003 (spent convictions)*
- *Listening Devices Act 1991*
- *Telecommunications (Interception) Tasmania Act 1999*[68]

The Personal Information Protection Act 2004 came into effect on 5 September 2005. It applies to the public and local government sectors and the University of Tasmania.[69]

The Act is a weakened form of the OECD model. It does not create a statutory office responsible for privacy matters, nor does it assign such responsibilities to any existing agency. A complaints-handling function is created, and assigned to the Ombudsman. (The practice in the State has been to consolidate all forms of review in the Ombudsman's Office, including FOI, police and health matters). The Ombudsman has no powers to enforce decisions.[70]

The only privacy-related information on the web-site appeared many months after the Ombudsman became responsible for privacy complaints.[71]

Privacy and personal information matters did not warrant mention in the Ombudsman's Annual Reports for 2004-05 or 2005-06.

Completion of PIAs

No evidence was found of any Tasmanian government agency having performed a PIA on any project or initiative.

[68] At: http://www.privacy.gov.au/privacy_rights/laws/#6 and http://www.privacy.org.au/Resources/PLawsST.html#Tas.
[69] At: http://www.austlii.edu.au/au/legis/tas/consol_act/pipa2004361/.
[70] At:http://www.ombudsman.tas.gov.au/.
[71] at: http://www.ombudsman.tas.gov.au/personal_information_protection.

VII. AUSTRALIAN CAPITAL TERRITORY

The Australian Capital Territory (A.C.T.) is a district which had a limited form of self-government imposed on it by the federal Parliament in the late 1980s. The city's population is about 300,000.

Legislative and Policy Framework

Legislation

Relevant laws include:

- *Human Rights Act 2004* (which includes a right to privacy*)*
- *Privacy Act 1988 (Cth)* [72]
- *Health Records (Privacy and Access) Act 1997*
- *Freedom of Information Act 1989*
- *Territory Records Act 2002 (*public records*)*
- *Spent Convictions Act 2000*
- *Listening Devices Act 1992*[73]

The A.C.T. is the only jurisdiction in Australia that has enacted a Bill of Rights – the Human Rights Act 2004. In s.12, the Act provides people with **a right to not have their privacy, family, home or correspondence interfered with unlawfully or arbitrarily.**[74]

The Act is administered by a Human Rights Commissioner with a small staff. There is nothing on the HRC's site to suggest that privacy is seen as a significant element of its responsibilities.[75]

A decade before the Human Rights Act was passed, the Territory chose to adopt the Commonwealth Privacy Act 1988. The authority for that is the Australian Capital Territory Government Service (Consequential Provisions) Act 1994 (which followed on from the 1988 Act that imposed self-government on the Territory), in particular s.23, Schedule 2 and Schedule 3.[76]

Among other things, this allocates to the federal Privacy Commissioner the responsibility to perform the functions of an A.C.T. Privacy Commissioner. The Office of the Federal Privacy Commissioner is located in Sydney, however. For some years there was a small office in Canberra, but that is no longer the case, and it appears that the responsibility may be worn lightly.

Within the A.C.T. Government, the primary responsibility for scrutiny of legislation for compliance with the Human Rights Act and the Privacy Act, and for advice on policy development, rests with the Department of Justice and Community Safety (JACS), and

[72] At: http://www.privacy.gov.au/privacy_rights/laws/#8.
[73] At http://www.privacy.gov.au/privacy_rights/laws/#8 and http://www.privacy.org.au/Resources/PLawsST.html#ACT.
[74] At: http://www.austlii.edu.au//au/legis/act/consol%5fact/hra2004148/.
[75] See: http://www.hrc.act.gov.au/.
[76] At: http://www.austlii.edu.au/au/legis/cth/consol_act/actgspa1994806/index.html.

in particular the Human Rights Unit. But other aspects of public law have to date absorbed the available resources.

PIA Guidance Material

No guidance appears to be provided to A.C.T. government agencies in relation to PIAs.

Completion of PIAs

No evidence was found of any A.C.T. government agency having performed a PIA on any project or initiative. In addition to the government handling a great deal of personal data relating to its residents generally, the Department of Corrective Services is preparing to impose continuous RFID-based tracking on prisoners in its new facility. It does not appear that a formal PIA has been undertaken into this initiative.

While no formal PIAs appear to be carried out, the Human Rights Unit advises that **new legislation is scrutinised against the Human Rights Act**, and this evaluation could reasonably be expected to extend privacy, including privacy of the person, personal behaviour and personal communications. On the other hand, this scrutiny appears to be largely internal dialogue within the A.C.T. public service, with limited public information and consultation.

IX. NORTHERN TERRITORY

The Northern Territory is a Territory with self-government powers, subject to occasional over-ride by the Commonwealth. It is about1.4 million square kilometers. (about the same as Portugal, Spain, France and Germany combined). It is mostly desert or semi-desert, and has a population of 200,000, about one-third indigenous. About 50% of the population lives in the capital city.

Policy and Legislation Framework

Legislation

Relevant Northern Territory relevant laws includes:[77]

- *Information Act 2002* (privacy, FOI and public records)
- *Criminal Records (Spent Convictions) Act 1992*
- *Surveillance Devices Act 2000*
- *Telecommunications (Interception) Northern Territory Act 2001*

A statute addressing both freedom of information and privacy was passed into law in 2002 and came into effect in mid-2003 as the Information Act (long title: An Act to provide for public access to information held by the public sector, to provide for the correction of personal information held by the public sector, to provide for the responsible collection and handling of personal information by the public sector, to promote appropriate records and archives management in the public sector, and for related purposes).[78] The Act created the statutory post of Information Commissioner.[79] It also provides for review after 5 years, and the review may extend to consideration of PIA matters.

Policy

No written guidance has yet been provided to agencies concerning PIAs. However, the Commissioner encourages agencies to discuss matters with the OIC, and some success has been achieved in this area.

In addition, in January 2007 mention of PIAs was made in the Commissioner's Submission to the Australian Law Reform Commission in relation to its review of federal privacy law. This is indicative of a general feeling among the four supervisory agencies that exist in Australian jurisdictions that the time has come for PIAs to be a mainstream activity, and for Commissioners to have powers that go beyond the provision of guidance (emphasis added).[80]

> "Presently the OPC [the Office of the federal Privacy Commissioner] provides a significant level of advice in relation to proposals that raise privacy issues. A requirement to obtain advice in relevant cases is set out in the Cabinet

[77] http://www.privacy.gov.au/privacy_rights/laws/#7 and http://www.privacy.org.au/Resources/PLawsST.html#NT.
[78] At: http://www.austlii.edu.au/au/legis/nt/consol_act/ia144/
[79] See Office of the Information Commissioner (OIC) websites at: http://www.privacy.nt.gov.au/ and http://www.nt.gov.au/justice/infocomm/privacy/index.shtml.
[80] See (pp. 25, 26) at http://www.nt.gov.au/justice/infocomm/docs/ntic_sub_on_dp31.pdf.

Handbook. However, there is no statutory requirement to consult the OIC about proposals.

"For agencies at least, it is worth considering whether that process should be formalised by inclusion of a requirement to consult the OPC in relation to any proposal that may raise privacy issues. The requirement could be general in nature or limited to legislative proposals.

"This would not necessarily require preparation of a privacy impact assessment for every proposal that raises privacy issues. In many cases, issues that arise might simply be dealt with by informal consultation with the OPC. The process could, however, be supplemented by **a power on the part of the OPC to direct that a privacy impact assessment be undertaken as part of the development process in an appropriate case**.

"Such a process would not preclude parliament or government from making legislation in the form that it sees fit. It would however, ensure that they are adequately informed in relation to potential privacy issues before deciding on whether to make the legislation..

"For existing legislation that impacts on privacy, consideration should also be given to requiring review, including consultation with the **OPC**, at regular intervals to ensure that any intrusions into the privacy of individuals are still warranted.

"**The OPC should have the following powers:**

- **direct that a privacy impact assessment be undertaken prior to implementation of the proposal;**
- **approve the terms of reference for the assessment (prepared by, and at the cost of, the proponent);**
- **review and comment on the assessment.**

"**All costs associated with the assessment should be met by the proponent.** There should be nothing to stop the OPC conducting an assessment if resources are available and the Commissioner considers it appropriate.

"**Any assessment conducted in relation to an agency proposal should be made public at an appropriate time.**

"Again, it should be stressed that the process would not preclude the parliament or the government from making laws in the manner it sees fit. It would however ensure that they are fully informed in relation to privacy issues.

Completion of PIAs

No evidence was found of any N.T. government agency having performed a PIA on any project or initiative.

However, the OIC has been involved in discussions about an initiative referred to as 'Territory Services'. This is considering a common shopfront as a way to reduce the number of government offices and consolidate citizen-facing resources. Because this has significant privacy implications, the Commissioner recommended that a PIA be performed, and provided the team developing the initiative with copies of the Australian and Victorian PIA Guidelines.