Government of South Australia

Privacy Committee
Of South Australia

Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2007

Executive Officer
Privacy Committee of South Australia
c/o State Records of South Australia
GPO Box 1072
ADELAIDE SA 5001
Phone (08) 8226 7750
privacy@saugov.sa.gov.au

September 2007

For information and advice, please contact:

The Presiding Member
Privacy Committee of South Australia
c/- State Records of South Australia
GPO Box 1072
ADELAIDE SA 5001

ph: (08) 8204 8786
fax: (08) 8204 8777
e-mail: privacy@saugov.sa.gov.au

This annual report has been issued pursuant to Clause 3 (1) of the Proclamation of the Privacy Committee of South Australia.

Government of South Australia

Privacy Committee
Of South Australia

The Hon Michael Wright MP
MINISTER FOR FINANCE

Dear Minister

The Privacy Committee of South Australia is pleased to provide you with this report of its activities for the year ending 30 June 2007. The report is provided pursuant to Clause 3(1) of the *Proclamation establishing the Privacy Committee of South Australia*, as amended and republished in the South Australian Government Gazette on 17 May 2001.

Terry Ryan
PRESIDING MEMBER
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

28 September 2007

Table of Contents

1 Introduction

This is the report of the activities of the Privacy Committee of South Australia (the Privacy Committee) for the year ending 30 June 2007. It has been prepared pursuant to Clause 3(1) of the Proclamation establishing the Privacy Committee (see Appendix B).

Similar to the previous year, this reporting year saw that the most prevalent issues coming before the members were related to data sharing, as the Government moves towards more seamless and efficient delivery of public services.

Agencies sought advice on how they could meet their privacy obligations as they collaborate with each other in initiatives that require personal information to be shared across the traditional departmental boundaries. The Privacy Committee was consulted on the privacy issues related to the data sharing required to deliver programs such as Street to Home and the Family Safety Framework. Involvement with these programs provided the Committee with valuable understanding to better respond more effectively to these types of enquiries.

As reported in previous years, inconsistency of privacy protection across Australia is still posing significant difficulties for members of the public and those responsible for privacy oversight. In this regard, the Privacy Committee has provided comments to the Australian Law Reform Commission (ALRC) as part of its review of the *Privacy Act 1988 (Cth)* (see item 3.2.1.1).

A number of enquiries this year have highlighted the gaps in privacy protection within South Australia. The local government, university and small business sectors are not bound to comply with any privacy protection regime, however some entities within these sectors are adopting privacy principles as a way of meeting customers' expectations. It is anticipated that recommendations from the ALRC, due to be presented in the first quarter of 2008, will point to potential solutions for some of these concerns.

During 2006-2007, the Privacy Committee granted three exemptions (see item 3.7), concluded three of six complaints (see item 3.6) and provided advice on privacy aspects of a number of programs and inquiries (see item 3.3). The Executive Support to the Committee responded to an increased number of telephone and email enquiries from the public and South Australian Public Sector agencies than in the previous year (see item 2.2.4).

The establishment of the Privacy Officer Network across Government (see item 3.4.1) is already showing results in increased efficiency when addressing privacy concerns within the South Australian Public Sector. The Network is proving very valuable when dealing with enquiries and complaints, as well as providing a forum for the dissemination of learnings from policy issues.

2 South Australian Public Sector Privacy Framework

2.1 The Information Privacy Principles

South Australia's Information Privacy Principles (IPPs) were introduced in July 1989 by means of *Cabinet Administrative Instruction 1/89*, issued as *Premier & Cabinet Circular No. 12*, and more commonly known as the Information Privacy Principles Instruction.

The IPPs regulate the way South Australian Public Sector agencies collect, use, store, and disclose personal information. A copy of the Information Privacy Principles Instruction can be found on the State Records website at www.archives.sa.gov.au/privacy, and in Appendix A of this report.

2.2 The Privacy Committee of South Australia

2.2.1 Establishment and Functions

The Privacy Committee of South Australia (the Privacy Committee) was established by proclamation in the Government Gazette on 6 July 1989. The functions of the Privacy Committee, as described in this Proclamation, are:

- to advise the Minister as to the need for, or desirability of, legislation or administrative action to protect individual privacy and for that purpose to keep itself informed as to developments in relation to the protection of individual privacy in other jurisdictions;
- to make recommendations to the Government or to any person or body as to the measures that should be taken by the Government or that person or body to improve its protection of individual privacy;
- to make publicly available information as to methods of protecting individual privacy and measures that can be taken to improve existing protection;
- to keep itself informed as to the extent to which the Administrative Scheme of Information Privacy Principles are being implemented;
- to refer written complaints concerning violations of individual privacy received by it (other than complaints from employees of the Crown, or agencies or instrumentalities of the Crown, in relation to their employment) to the appropriate authority;
- such other functions as are determined by the Minister.

These functions use terminology that is broader than Information Privacy. The functions are also not necessarily restricted to activity within the South Australian Public Sector. However the level of resourcing (see item 2.2.4) necessitates a focus on matters that carry the greatest impact on the application of the IPPs, and the handling of personal information within the South Australian Public Sector.

A copy of the Proclamation can be found following the Information Privacy Principles Instruction, and in Appendix B of this report.

2.2.2 Reporting

The Privacy Committee reports to the Minister for Finance, the Hon Michael Wright MP.

2.2.3 Membership

There are six members:

- three nominated by the Minister responsible (one of whom is not a public sector employee and one of whom will have expertise in information and records management)
- one nominated by the Attorney-General
- one nominated by the Minister for Health
- one nominated by the Commissioner for Public Employment.

For this reporting year, the Privacy Committee comprised:

Presiding Member:

- Terry Ryan, Director, State Records of South Australia, Department of the Premier and Cabinet

Members, in alphabetical order:

- Gaby Jaksa, Commercial Counsel, Crown Solicitor's Office (resigned November 2006)
- Grantly Mailes, Chief Information Officer, Government of South Australia (commenced December 2006)
- Bernadette Quirke, Senior Solicitor, Crown Solicitor's Office, Attorney-General's Department
- Nancy Rogers, Manager, Research & Analysis, Department for Families and Communities
- Andrew Stanley, Director, Strategic Planning, Policy and Research, Department of Health
- Lee Thomas, non-public sector employee, and Branch Secretary, South Australian Branch of the Australian Nursing Federation.

The term of appointment for each of the current members expires on 9 November 2006.

2.2.4 Resources

State Records of South Australia provides resources for the Privacy Committee. This facilitates support to the Privacy Committee, including research and advisory support and a public enquiry service. The resources include the commitment of time from various personnel, forming the equivalent of approximately 1.0 FTE.

The public enquiry service responds to telephone and e-mail enquiries relating to privacy of personal information in South Australia. There were approximately 320 telephone and e-mail enquiries received during the reporting year, which was an increase of 45% from the previous reporting year.

Throughout the year, State Records delivered Privacy Awareness Training for South Australian State and Local Government agencies. Privacy management has been included in the curriculum for the nationally accredited Certificate III in Business (Recordkeeping), developed and delivered by State Records.

Premier & Cabinet Circular No. 16: Remuneration for Government Appointed Part-time Boards and Committees specifies the conditions under which members of Boards and

Committees may be paid. In general, fees are not paid to Government employees, and so only one member of the Privacy Committee receives a sessional fee. The sessional fees are drawn from State Records' recurrent operating budget. For more information about the payment of fees, see *Premier & Cabinet Circular No. 16* available at www.premcab.sa.gov.au/pdf/circulars/Remuneration.pdf.

2.2.5 Meetings

During the reporting year the Privacy Committee met on seven occasions. Meetings were supplemented by the conduct of business out of session.

2.2.6 Guidelines for members

A handbook for members contains information on the role of the Privacy Committee, its relationship to other approval and advisory bodies, duties and obligations of members, the process for handling complaints, and other information of value to members in performing their role. It contains a brief history of privacy law and self-regulation in South Australia, and an overview of the protection of personal information in other jurisdictions. The handbook also contains a Code of Conduct for members that is consistent with *Government Boards and Committees: Guidelines for Agencies and Board Directors* (Department of Premier and Cabinet, 2000).

A copy of the handbook can be found on the State Records website at www.archives.sa.gov.au/privacy/committee.html.

2.2.7 South Australia's Strategic Plan

South Australia's Strategic Plan 2007 (the Strategic Plan) calls for performance improvement across the South Australian public sector by improvement in government decision-making and administrative efficiency (South Australia's Strategic Plan Objective 1: Growing Prosperity: Targets T1.8 and T1.9). The Privacy Committee continues to improve in this area by implementing strategies such as out of session conduct of business. Since the establishment of the Privacy Officer Network some efficiencies have also been achieved in the handling of complaints and enquiries from members of the public.

The constitution of the Privacy Committee meets Target T5.1 (Objective 5: Building Communities) to *'increase the number of women on all State Government boards and committees to 50% on average by 2008'*. During the reporting year the Privacy Committee had 50% female membership.

The activities of the Privacy Committee are critical to the achievement of other Strategic Plan targets and priority actions across the South Australian Public Sector. Examples include:

- Objective 1: Growing Prosperity: Target T1.7: *'performance in the public sector – customer and client satisfaction with government services'* – the Australian public expects a high degree of privacy protection when accessing government services, and also expect a degree of control over how their personal information will be collected, stored, used and disclosed[1].
- Objective 2: Improving wellbeing: all targets – there is a need for research and development in the areas of health, wellbeing and public safety, including the evaluation of programs designed to deliver these targets. The use of personal information for research requires close attention to application of the IPPs.

- Objective 5: Building Communities: Priority Actions: *'collaborate to improve access to services [and] increase … resource sharing'*; and Objective 6: Expanding opportunity: all targets – there has been an marked increase in data matching and sharing activities, that presents a challenge for agencies in adherence to their obligations over personal information.

3 Activities of the Privacy Committee

3.1 Advice to the Minister

The Privacy Committee has the function, under clause 2(a) of the Proclamation, *'to advise the Minister as to the need for, or desirability of, legislative or administrative action to protect individual privacy'*.

The Privacy Committee briefed the Minister on matters relating to privacy, primarily through submissions to national programs and inquiries.

3.2 Developments in other jurisdictions

The Privacy Committee has the function, under clause 2(a) of the Proclamation, *'to keep itself informed of developments in relation to the protection of individual privacy in other jurisdictions'*. Some key instances are described below.

3.2.1 Commonwealth, States and Territories

The Commonwealth and each State and Territory Government within Australia operate under varying legislative and policy regimes for privacy protection. These regimes are of interest to the Privacy Committee as it considers its own responses to local and national issues. The following presents some of the more significant developments in other jurisdictions that have been noted by the Privacy Committee.

3.2.1.1 Australian Law Reform Commission Review of the Commonwealth Privacy Act

The Australian Law Reform Commission (ALRC) commenced a review of the Commonwealth *Privacy Act 1988* (the Cth Privacy Act) in 2006. The Cth Privacy Act applies to Commonwealth Government Departments and most private businesses, including all private health care providers in Australia. It does not apply to State and Territory Government Agencies, Local Government Authorities, Universities or some small businesses. The review is considering relevant existing Commonwealth, State and Territory laws and practices, constitutional issues and other matters.

The Privacy Committee provided comments through the Minister, which helped form part of the South Australian Government's submission to the ALRC's *Issues Paper 31: Review of Privacy* on 12 February 2007 and representatives of the Committee met with the Commissioner on 1 March 2007. A discussion paper that will include recommendations is due for release in September 2007. The Privacy Committee will consider the recommendations and if appropriate will prepare a response. The review is to be completed by 31 March 2008.

3.2.1.2 National Identity Security Strategy

On 13 April 2007, the Council of Australian Governments (COAG) signed an agreement for the development and implementation of a National Identity Security Strategy (NISS) to better protect the identities of Australians.

The strategy will aim to enhance identification and verification processes and develop other measures to combat identity crime and is underpinned by the inter-governmental agreement, which includes:

- the development and implementation of a national document verification service to combat the use of false and stolen identities;
- investigation of the means by which reliable, consistent and nationally interoperable biometric security measures could be adopted by all jurisdictions; and
- ensuring the quality of databases.

A National Identity Security Coordination Group (Coordination Group) has been established to develop the NISS and oversee its implementation.

During the consultation process in the lead-up to the April COAG meeting, the Privacy Committee raised a number of issues that reflected the complexity of identity management and the significance and potential impact of the Agreement. The issues included:

- the resourcing impact for South Australian Government agencies, State Records and the Privacy Committee to implement the National Identity Security Strategy;
- the membership of the National Coordination Group in regard to the lack representation of privacy at a State or Territory level;
- the complexity of managing identity information when biometric information is included;
- the adequacy of the Privacy Regime in South Australia to meet the requirements of the Agreement; and
- whether current State legislation is adequate to deal with the collection of biometrics and biometric information.

The Privacy Committee will continue to keep itself informed about the NISS coordination process, as appropriate.

3.2.1.3 Other Commonwealth and National initiatives

This reporting year saw an unprecedented volume of material emanating from Commonwealth Government and federal initiatives that have the potential to impact South Australian Public Sector agencies' management of personal information. In particular, the following matters attracted the Privacy Committee's attention:

- Amendments to the Commonwealth *Privacy Act 1988* – emergency and disaster provisions. It was recognised that some provisions interrelate with South Australian emergency management law.
- The Commonwealth Government's proposed Human Services Access Card – two draft Bills, released for public comment in June 2007, aim to facilitate the introduction of an Access Card, and change how people access Medicare and Australian Government benefits.
- The Commonwealth Government's e-Authentication Framework for Individuals – this framework holds some relationship to the National Identity Security Strategy and the Commonwealth Human Services Access Card. As such, many of the issues raised by the Privacy Committee are similar.

3.2.2 Conferences and seminars

Throughout the year, representation of the Privacy Committee at various conferences, seminars and forums, included:

- State Records Biennial Conference: *Digital Future: deliverance from dysfunction*, 21-22 November 2006.
- Privacy Breakfast Forum, hosted by the Commonwealth Privacy Commissioner, Adelaide, 10 May 2007.
- Asia Pacific Privacy Authorities (APPA), Cairns, Queensland, 22-23 June 2007.

3.2.2.1 Asia Pacific Privacy Authorities

Asia Pacific Privacy Authorities (APPA) group convenes twice a year with meetings hosted on a rotating basis by the various Privacy Commissioners. At the forum, issues are discussed such as privacy and security, identity management, surveillance, cross-jurisdictional law enforcement between countries in the Pacific Rim, privacy legislation amendments, cryptography and personal data privacy.

A representative of the Privacy Committee attended the meeting on 22-23 June 2007 in Cairns, Queensland. At that meeting, various jurisdictional reports were provided. Key points from the reports included advice on the introduction of new privacy legislation, the progress of current inquiries, appointments to senior positions, and various measures that have been adopted to raise the profile of privacy.

3.3 Recommendations and submissions

The Privacy Committee has the function, under clause 2(b) of the Proclamation, *'to make recommendations to the Government or to any person or body as to the measures that should be taken by the Government or that person or body to improve its protection of individual privacy'*.

The Privacy Committee responded to various requests for advice, support and recommendations. Key instances are described below.

3.3.1 Review of the Information Privacy Principles

The Privacy Committee submitted a proposal to the Minister in May 2005 to vary the IPPs to recognise the activity of contracting for services. Work on the proposal, in particular in relation to the development of model contractual terms and conditions, has been underway throughout the reporting year, and continues into the next.

3.3.2 Street to Home Service

It was reported in the Annual Report for the year ending 30 June 2006 that the Central Northern Adelaide Health Service (CNAHS) had approached the Privacy Committee in December 2005 for advice regarding the sharing of client information for a Social Inclusion initiative called Street to Home Service. This service is central to the State Government's response to homeless people in the inner city and involves a collaborative approach between various entities delivering services to homeless people. The collaborative approach calls for sharing of personal information between services.

The Privacy Committee advised that Principle 10(b) of the IPPs allows relevant third parties to share information where required *'to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person'*. The Privacy Committee advised CNAHS and the Social Inclusion Unit that, in the context of the briefing provided, the Privacy Committee considered that the proposed sharing of information would generally fall within this exception and therefore approval to disclose or share information would not, generally, be required. The Privacy Committee

confirmed this view in discussions and communications with CNAHS and the Social Inclusion Unit during the current reporting year.

The contextual application of terms such as 'reasonable', 'imminent' and 'serious' are critical to the interpretation and applicability of this exception.

3.3.3 Release of Drivers License Records to the Australian Electoral Commission

In September 2006, the Department for Transport, Energy and Infrastructure (DTEI) approached the Privacy Committee with information about amendments to the *Electoral Act 1918 (Cth)*. Once enacted, the Australian Electoral Commission (AEC) would be able to gain access to all State and Territory drivers' license information to verify electoral claims. The information is to be provided through Austroads, the association of Australian and New Zealand road transport and traffic authorities.

Advice from other jurisdictions had been sought through Austroads, including legal advice on the impact of the recent amendments on another jurisdiction's Motor Registration law. The legal advice raised a question as to whether South Australia's *Motor Vehicles Act 1959* could allow the information disclosure to take place in the way it had been requested by the AEC. It was the Privacy Committee's view that there were privacy concerns in the use (under IPP 8) and disclosure (under IPP 10) of this information and that there were also intergovernmental issues that might not have been fully considered. The Privacy Committee sought further information from DTEI regarding advice obtained from the Crown Solicitor's Office and Privacy Commissioners.

It was found that there was no legal impediment to the disclosure of the information, the Privacy Committee advised that the disclosure was able to take place for the purposes of complying with a law. However, the Privacy Committee advised DTEI that some concerns remained as to the scope of the information disclosure, and whether it would involve records relating to individuals of no interest to the AEC (ie those licensed to drive who are ineligible to vote). Recommendations were made for points to be included in any Memorandum of Understanding that would facilitate the information disclosure.

3.3.4 Release of Drivers License Photographs to Police

In October 2006, the Privacy Committee considered a request for advice from the Department for Transport, Energy and Infrastructure (DTEI) regarding proposed amendments to the *Motor Vehicles Act 1959*, which would allow the disclosure of photographs held by the Registrar of Motor Vehicles to South Australia Police (SAPOL) for criminal investigations involving serious offences.

The Privacy Committee's view was that, provided the proposed amendments did not go beyond the extent of disclosure generally supported by the IPPs, particularly IPP 10(d), there was no privacy concern. Disclosure, as necessary to enforce the criminal law, is permitted within IPP 10(d).

3.3.5 Student Truancy Scheme

In the previous reporting year, the Privacy Committee wrote to the Department of Education and Children's Services (DECS) to seek advice on a proposal to issue pass-cards to school students as part of a truancy management scheme. Of particular interest was whether the scheme would require the collection of new personal information from students.

During this reporting year, a response from DECS satisfied the Privacy Committee that the scheme was compliant with IPPs 2 and 8. The Privacy Committee responded that it would be good practice to proactively advise parents of the scheme and how the information is handled, and that doing so would support compliance with IPP 2.

DECS subsequently responded to the Privacy Committee that it requires parents and carers to advise the school of reasons for any absence for their child. DECS also believes the placement of the Privacy Statement prominently on a recently amended enrolment form complies with the recommendation to proactively advise parents of the program. The Privacy Committee noted the response.

3.3.6 School Student Enrolment Form

In 2005, the Privacy Committee wrote to the Department of Education and Children's Services (DECS) to seek advice on recent amendments to the primary and secondary school student enrolment forms. The Privacy Committee was concerned from reports that a new school enrolment form was being used to collect additional information, about both students and parents, than had previously been sought.

DECS' response advised that the collection of additional information was required in order to meet Commonwealth Government reporting requirements, and therefore satisfies the requirements of IPPs 2 and 10. DECS proposed to clarify the privacy statement on the form. In support of the idea, the Privacy Committee sought further advice regarding the reporting requirements and recommended restructuring the form to make clear the information that was required by whom and under what authority.

During this reporting year, the structure of the form and the content of the privacy statement were agreed upon.

3.3.7 Public Access to Archival Records

In March 2007, State Records of South Australia consulted with the Privacy Committee on a proposed upgrade and amendment of the *Public Access Determinations Guideline*. The Guideline provides advice to agencies and guidance for State Records relating to the administration of public access to official records in the custody of State Records. Section 26 of the *State Records Act 1997* requires the agency responsible for an official record in the custody of State Records to determine conditions of public access to records.

Recent amendments to the *Freedom of Information Act 1991* removed the time period of 30 years where a document ceases to be exempt because it contains personal information. This means that a document containing personal information can no longer be released under the *Freedom of Information Act 1991*, regardless of its age, unless it is reasonable to do so. The Guideline has been revised to reflect this amendment and to take into consideration a reasonableness test. Records that contain low-level personal information would therefore be open to public access after 30 years, if containing medium-level personal information after 60 years and all records of a personal nature, irrespective of the level of information, should be open after 100 years.

The Guideline, by its nature, recognizes that privacy diminishes with time and ceases upon the death of the individual. The Privacy Committee supported the Guideline, subject to some recommendations about its implementation.

3.3.8 Health Data Linkage

The Department of Health sought advice from the Privacy Committee on a proposal to implement a de-identified health data linkage initiative. The Privacy Committee agreed that the proposal had merit as long as the method for data linkage was used for case-by-case research proposals with ethics committee approval and not for large-scale profiling. The methodology was based on a model used by the Western Australian Government, which uses technology to minimise the risk of unauthorized disclosure of personal information.

3.4 Communication

The Privacy Committee has the function, under clause 2(c) of the Proclamation, *'to make publicly available, information as to methods of protecting individual privacy and measures that can be taken to improve existing protection'*.

3.4.1 Privacy Officer Network

The inaugural and second meetings of the Privacy Officer Network were held on 8 September 2006 and 21 May 2007. The Network, coordinated by State Records, aims to increase the efficiency of communications about the handling of personal information held by the South Australian Public Sector, and to assist Principal Officers of agencies to fulfill their obligation to comply with the IPPs.

The Network is contributing to a more robust culture of privacy awareness across the Public Sector.

3.4.2 Participation in committees and groups

When the opportunity arises, the Privacy Committee is represented at meetings with Commonwealth, State and Territory Governments as deemed appropriate.

The Privacy Committee is represented on the Department of Health Ethics and Privacy Committee, the Justice Information Systems Privacy Committee, the South Australian Identity Security and Management Group and the Asia Pacific Privacy Authorities (APPA) forum (see also item 3.2.2.1).

3.5 Keep informed as to the extent to which the Information Privacy Principles are implemented

The Privacy Committee has the function, under clause 2(d) of the Proclamation, *'to keep itself informed as to the extent to which the Administrative Scheme of Information Privacy Principles are being implemented'*.

The Privacy Committee does seek reports from agencies from time to time. See section 3.3 (Recommendations and submissions) for reviews and reports.

3.6 Complaints

The Privacy Committee has the function, under clause 2(e) of the Proclamation, *'to refer written complaints concerning violations of individual privacy received by it (other than complaints from employees of the Crown, or agencies or instrumentalities of the Crown, in relation to their employment) to the appropriate authority'*.

Three new complaints were received this reporting year, and three pre-existing written complaints underwent further deliberation. Of the six complaints handled this year, three were concluded and three remain outstanding.

Of the three completed complaints, one involved personal information handling activities allowed under specific legislation. In the other two, it was not clear whether or not a breach of the IPPs occurred, based on the facts provided. In one of these cases, the Committee made recommendations to the agency concerned to ensure clients are given more adequate guidance on the way personal information is handled.

The information involved fell into the subject areas of professional registration, law enforcement / criminal investigation, and the handling of criminal history details.

3.7 Exemptions

The Privacy Committee may, under clause 4 of the Proclamation, *'exempt a person or body from one or more of the Information Privacy Principles (IPPs) on such conditions as the Privacy Committee thinks fit'*.

Requests for exemptions are addressed on a case-by-case basis. Exemptions, in practice, are only applied in situations where the public interest for an activity outweighs the privacy protections afforded by the IPPs, or where otherwise warranted by unique circumstances. Exemptions are generally subject to conditions, and agencies are often asked to report on the activity conducted under the exemption.

The *Code of Fair Information Practice*, approved by the Privacy Committee for use within the Department of Health and Department for Families and Communities, contains provisions allowing use of personal health information for research purposes, but excludes non-health information. *Cabinet Administrative Instruction 1/89* does not contain a provision for the use of personal information for research purposes.

During this reporting year, six exemptions were considered and three were approved. Following is a summary of each of the requests for exemption.

3.7.1 Office of Crime Statistics and Research: collect, use and disclose personal information for the purposes a research project

During the previous reporting year, the Privacy Committee considered a request for exemption, from IPPs 2 and 10, from the Office of Crime Statistics and Research (OCSAR), to allow collection and disclosure of personal information for the research project *A comparative analysis of Violence Intervention Program (VIP) and non-VIP clients referred from the Family Violence Courts*. The request was to allow personal information about clients to be collected by OCSAR without obtaining the clients' consent. At the time, the Privacy Committee determined that the collection of the personal information would have caused a breach of confidence because the clients received a confidentiality undertaking when they entered the program.

The Privacy Committee agreed to reconsider the exemption should further information be supplied by OCSAR in support of the program. OCSAR approached the Privacy Committee in December 2006 seeking reconsideration. The request for exemption was refused again on the grounds of potential breach of confidence.

The Privacy Committee advised OCSAR that program managers should use a modified consent form which seeks consent to use personal information for program evaluation.

3.7.2 Department of Trade and Economic Development: use of contact information of graduates of South Australian universities now residing interstate

The Department of Trade and Economic Development (DTED) sought an exemption from IPP 8 regarding the use of information already held by DTED to market South Australia to graduates of South Australian universities now residing interstate.

The Privacy Committee expressed concern that the purpose for which the information was to be used was not the same as the purpose for which the information was collected by DTED. However it was recognised that the purpose was related, and therefore members approved the exemption, on the condition that it was recognised to be a one-off approval, and that all recipients of the marketing material would be able to opt-out from receiving future correspondence.

See Appendix C for the full text of the exemption.

3.7.3 Office of Crime Statistics and Research and South Australian Police Department: sharing of unit record data for criminological research and evaluation

A Memorandum of Understanding (MoU) was developed between South Australia Police (SAPOL) and the Office of Crime Statistics and Research (OCSAR), both agencies of the Attorney-General's Department, which aimed to share police unit record information in order to[2]:

- provide timely, accurate and comprehensive statistical information on crime and criminal justice, with particular focus on providing relevant data for policy development and legislative change;
- conduct research into crime and criminal justice issues, including evaluations of the impact of legislative change and the introduction of new criminal justice practices; and
- disseminate information on crime and criminal justice to the Government, members of Parliament, relevant agencies and the community in order to increase the general level of understanding and to inform public debate and policy development in these areas.

The Privacy Committee advised the Attorney-General's Department that exemption from IPPs 2, 8 and 10 would be required to allow the proposed activities to take place. SAPOL and OCSAR subsequently submitted requests to be able to share the personal information between the two agencies.

The Privacy Committee approved two exemptions – one from IPP 10 to allow SAPOL to disclose the information to OCSAR, and the other from IPPs 2 and 8 to allow OCSAR to collect and use the information. See Appendix D for the full text of the two exemptions. A synopsis of the MoU is available upon request.

3.7.4 Department of Further Education, Employment, Science and Technology: Construction Industry Training Board

The Department of Further Education, Employment, Science and Technology (DFEEST), sought an exemption from IPP 10 to allow disclosure of trainee and employer contact information by DFEEST to the Construction Industry Training Board (CITB), for the purpose of advertising scholarships to trainees and employers.

The exemption was refused on the grounds that as DFEEST holds the information, it was therefore more appropriate that DFEEST be the distributor of the invitation to apply for a

scholarship. Subsequent to the refusal, representatives of the Privacy Committee met with representatives of DFEEST and CITB, in order to canvas alternative options for information flow to active trainees and their employers.

3.7.5 Office for Women et al: Family Safety Framework

The Office for Women sought advice from the Privacy Committee, on whether or not an exemption might be required from the IPPs to allow information sharing between specified agencies for the operation of a Family Safety Framework. The Family Safety Framework was developed by the Women's Safety Strategy Whole of Government Reference Group, to respond to high-risk cases of interpersonal violence involving women, children and young people. It was planned to involve key agencies in the sharing of information at Family Safety Meetings for the purpose of protecting women, children and young people from serious injury or death.

As the Framework is based on a need to share personal information to prevent or lessen a serious or imminent threat to the health or life of individuals, for the most part, operations of the Framework will not breach the IPPs. The Privacy Committee supported the proposal and advised that no exemption was required.

The Office for Women subsequently asked for further advice regarding expansion of the Framework to include non-government organisations (NGOs) involved in providing domestic violence support services on behalf of Government. The Privacy Committee agreed that the involvement was appropriate, provided that the Government's relationship with the NGOs was recognised under a contractual agreement, and that the agreement particularly addressed issues such as physical security of the information and staff training. The Privacy Committee also agreed that the National Privacy Principles, as expressed under the *Code of Fair Information Practice*, should apply. In cases where the NGO is currently bound under the Commonwealth *Privacy Act 1988*, compliance will be harmonious with many of the compliance obligations under that Act.

Endnotes:

[1] *Community Attitudes to Privacy* surveys, commissioned by the Office of the Privacy Commissioner, Australia in 2001, 2004, and 2007. Publications are available at www.privacy.gov.au.

[2] Objectives taken from the Memorandum of Understanding. See Appendix D.

Appendices

A Information Privacy Principles

A link to this document can be found on the Department of Premier and Cabinet website at www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf.

Cabinet Administrative Instruction No.1 of 1989

(Premier and Cabinet Circular No. 12)

(Re-issued 30 July 1992)

PART 1

PRELIMINARY

Short Title

1. This Instruction may be called the *'Information Privacy Principles Instruction'*.

Commencement and Application

2. (1) This Instruction will come into effect on 30 July, 1992.

   (2) Subject to any contrary determination by Cabinet, this Instruction shall apply to–

      (i) 'the public sector' as that expression is defined in Section 4 (1) of the *Government Management and Employment Act 1985*: and

      (ii) any agency or instrumentality of the State of South Australia that is subject to control or direction by a Minister.

   (3) This Instruction shall not apply to an agency that appears in the attached schedule.

Interpretation

3. (1) In this Instruction –

   'agency' means an agency that falls within the scope of application of this Instruction pursuant to the provisions of Clause 2 (2):

   'the Committee' means the Privacy Committee of South Australia constituted by Proclamation.

   'personal information' means information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

   'principal officer' means in relation to an agency:

   (a) the person holding, or performing duties of, the Office of Chief Executive Officer of the agency;

(b) if the Government Management Board declares an office to be the principal office in respect of the agency – the person holding, or performing the duties of, that office; or

(c) in any other case – the person who constitutes that agency or, if the agency is constituted by two or more persons, the person who is entitled to preside at any meeting of the agency at which the person is present:

'the Principles' means the Information Privacy Principles established under Clause 4 of this Instruction:

'record-subject' means a person to whom personal information relates.

PART II

INFORMATION PRIVACY PRINCIPLES

Principles

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:

Collection of Personal Information

(1) Personal information should be not collected by unlawful or unfair means, nor should it be collected unnecessarily.

(2) An agency that collects personal information should take reasonable steps to ensure that, before it collects it or, if that is not practicable, as soon as practicable after it collects it, the record subject is told:

(a) the purpose for which the information is being collected (the 'purpose of collection'), unless that purpose is obvious;

(b) if the collection of the information is authorised or required by or under law – that the collection of the information is so authorised or required; and

(c) in general terms, of its usual practices with respect to disclosure of personal information of the kind collected.

(3) agency should not collect personal information that is inaccurate or, having regard to the purpose of collection, is irrelevant, out of date, incomplete or excessively personal.

Storage of Personal Information

(4) An agency should take such steps as are, in the circumstances, reasonable to ensure that personal information in its possession or under its control is securely stored and is not misused.

Access to Records of Personal Information

(5) Where an agency has in its possession or under its control records of personal information, the record-subject should be entitled to have access to those records in accordance with the *Freedom of Information Act 1991*.

Correction of Personal Information

(6) An agency that has in its possession or under its control records of personal information about another person should correct it so far as it is inaccurate or, having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, incomplete, irrelevant, out of date, or where it would give a misleading impression in accordance with the *Freedom of Information Act 1991*.

Use of Personal Information

(7) Personal information should not be used except for a purpose to which it is relevant.

(8) Personal information should not be used by an agency for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose unless:

(a) the record-subject has expressly or impliedly consented to the use;

(b) the agency using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person.

(c) the use is required by or under law; or

(d) the use for that other purpose is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer.

(9) An agency that uses personal information should take reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up to date.

Disclosure of Personal Information

(10) An agency should not disclose personal information about some other person to a third person unless:

(a) the record-subject has expressly or impliedly consented to the disclosure;

(b) the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person;

(c) the disclosure is required or authorised by or under law; or

(d) the disclosure is reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer.

Acts and Practices of, and Disclosure of Information to Staff of Agency Etc.

5. For the purposes of this Instruction –

(a) an act done or practice engaged in by, or personal information disclosed to, a person employed by, or in the service of, an agency in the performance

of the duties of the person's employment shall be deemed to have been done or engaged in by, or disclosed to, the agency;

(b) an act done or practice engaged in by, or personal information disclosed to, a person on behalf of, or for the purposes of the activities of, an unincorporated body. being a board, council, committee, subcommittee or other body established by, or in accordance with, an enactment for the purpose of assisting, or performing functions in connection with, an agency, shall be deemed to have been done or engaged in by, or disclosed to, the agency.

Agencies to comply with Principles

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.

Collecting of Personal Information

7. For the purposes of the Principles, personal information shall be taken to be collected by an agency from a person if the person provides that information to the agency in response to a request by the agency for that information or for a kind of information in which that information is included.

PART III

COMPLIANCE WITH PRINCIPLES

8. The Committee may at any time on its own initiative appoint a person (whether or not that person is a public employee) or the Commissioner for Public Employment to investigate or assist in the investigation of the nature and extent of compliance of an agency with the Principles and to furnish a report to the Committee accordingly.

Reporting Procedures Pursuant to this Instruction

9. Each principal officer shall furnish to the Committee such information as the Committee requires and shall comply with any requirements determined by the Committee concerning the furnishings of that information including:

(a) the action taken to ensure that the Principles are implemented, maintained and observed in the agency for which he or she is responsible;

(b) the name and designation of each officer with authority to ensure that the Principles are so implemented, maintained and observed;

(c) the result of any investigation and report, under Clause 8, in relation to the agency for which he or she is responsible and, where applicable, any remedial action taken or proposed to be taken in consequence.

Agencies Acting Singly or in Combination

10. This Instruction and the Principles shall apply to the collection, storage, access to records, correction, use and disclosure in respect of personal information whether that personal information is contained in a record in the sole possession

or under the sole control of an agency or is contained in a record in the joint or under the joint control of any number of agencies.

SCHEDULE: CLAUSE 2 (3)

Agencies to which this Instruction does not apply

State Government Insurance Commission
Workers' Rehabilitation and Compensation Corporation

B Proclamation of the Privacy Committee of South Australia

A link to this document can be found as an addendum to the Information Privacy Principles link on the Department of Premier and Cabinet website at www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf.

I, the Governor, with the advice and consent of the Executive Council proclaim as follows:

Establishment of Privacy Committee of South Australia

1. (1) The Government will establish a committee to be known as the Privacy Committee of South Australia.

(2) The Committee will consist of six members appointed by the Minister as follows:

(a) three will be chosen by the Minister, and of these one must be a person who is not a public sector employee (within the meaning of the *Public Sector Management Act 1995*) and one must be a person with expertise in information and records management;

(b) one will be appointed on the nomination of the Attorney-General;

(c) one will be appointed on the nomination of the Minister for Human Services;

(d) one will be appointed on the nomination of the Commissioner for Public Employment.

(2a) One of the persons appointed under subclause (2)(a) will be appointed (on the nomination of the Minister) to be the presiding member.

(3) A member will be appointed for a term not exceeding four years.

(3a) Where a member is appointed for a term of less than four years, the Minister may, with the consent of the member, extend the term of the appointment for a period ending on or before the fourth anniversary of the day on which the appointment took effect.

(4) The office of a member becomes vacant if the member —

(a) dies;

(b) completes a term of office and is not reappointed;

(c) resigns by written notice to the Governor; or

(d) is removed from office by the Governor on the ground of —

(i) mental or physical incapacity to carry out official duties satisfactorily;

(ii) neglect of duty;

(iii) disclosure of information by the member contrary to clause 3 (2); or

(iv) misconduct.

(5) —

(a) A meeting of the Committee will be chaired by the presiding member or, in his or her absence, by a member chosen by those present.

(b) Subject to paragraph (c), the Committee may act notwithstanding vacancies in its membership.

(c) Four members constitute a quorum for a meeting of the Committee.

(d) A decision in which a majority of the members present at a meeting concur is a decision of the Committee but if the members are equally divided the person presiding at the meeting will have a casting vote.

(e) A member who is unable to attend a meeting of the Committee may, with the approval of the presiding member, be represented for voting and all other purposes at the meeting by his or her nominee.

(f) Subject to this subclause the Committee may determine its own procedures.

(g) The Committee must keep minutes of its proceedings.

(6) In performing its functions the Committee may consult any person and may establish subcommittees of at least two of its members to assist and advise it.

Functions of the Committee

2. The Committee will have the following functions:

(a) to advise the Minister as to the need for, or desirability of, legislation or administrative action to protect individual privacy and for that purpose to keep itself informed as to developments in relation to the protection of individual privacy in other jurisdictions;

(b) to make recommendations to the Government or to any person or body as to the measures that should be taken by the Government or that person or body to improve its protection of individual privacy;

(c) to make publicly available information as to methods of protecting individual privacy and measures that can be taken to improve existing protection;

(d) to keep itself informed as to the extent to which the Administrative Scheme of Information Privacy Principles are being implemented;

(e) to refer written complaints concerning violations of individual privacy received by it (other than complaints from employees of the Crown, or agencies or instrumentalities of the Crown, in relation to their employment) to the appropriate authority;

(f) such other functions as are determined by the Minister.

General

3. (1) The Committee must prepare a report of its activities annually in accordance with section 66 of the *Public Sector Management Act 1995* and must submit the report to the Minister as required by that section;

(2) A member of the Committee must not disclose any information acquired by the member by virtue of his or her membership of the Committee except —

(a) in the course of performing duties and functions as a member of the Committee; or

(b) as required or authorized by law.

4. (1) The Committee may exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Committee thinks fit.

(2) The Committee must include details of exemptions granted under subclause (1) in its annual report.

5. In this proclamation, unless the contrary intention appears —

‘Information Privacy Principles’ means the principles set out in Part II of Cabinet Administrative Instruction No. 1 of 1989 entitled ‘Information Privacy Principles Instruction’;

‘Minister’ means the Minister who is, for the time being, responsible for the Committee.

Established 6 July 1989; amended 30 July 1992, 25 May 2000 and 17 May 2001 by proclamation in the Government Gazette.

C Exemption Granted – Department for Trade and Economic Development

See also item 3.7.2.

EXEMPTION FROM COMPLIANCE WITH THE INFORMATION PRIVACY PRINCIPLES

In accordance with Clause 4 of the Privacy Committee's Proclamation the following exemption from *Cabinet Administrative Instruction 1/89 'The Information Privacy Principles'* (the IPPs) is granted.

This applies to the Department of Trade and Economic Development (DTED), allowing use of personal information about approximately 350 graduates of South Australian Universities who currently reside interstate, for the purpose of conducting a survey. The personal information comprises contact information provided by the graduates to DTED in response to an invitation to Alumni events during 2006.

The exemption is dependent upon the condition that correspondence with the graduates should include an opt-out from receiving further correspondence from DTED.

This exemption will expire twelve (12) months from approval, or upon completion of the survey project, whichever is sooner.

[Original signed]

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
29 December 2006

Approval granted by Privacy Committee of South Australia on 6 December 2006

D Exemptions Granted – Office of Crime Statistics and Research and South Australia Police

See also item 3.7.3.

Exemption for South Australia Police

In accordance with Clause 4 of the Privacy Committee's Proclamation the following exemption from *Cabinet Administrative Instruction 1/89 'The Information Privacy Principles'* is granted.

This exemption applies to the South Australia Police (SAPOL). It is an exemption from compliance with Principle 10, allowing disclosure of personal information to the Office of Crime Statistics and Research (OCSAR) for that personal information to be used for the purposes of statistical monitoring, research and evaluation projects. Conditions apply.

All other Principles continue to apply.

Compliance

The Principal Officer of SAPOL must ensure compliance with this exemption.

Conditions

This authorisation for disclosure of personal information is conditional.

The personal information to be disclosed is described in the Memorandum of Understanding (MoU) between OCSAR and SAPOL. A synopsis of the MoU is available upon request. Broadly, it includes:

- extracts from SAPOL of unit record data from the Police Incident Management System;
- access to the SAPOL General Enquiry Information System in the Justice Information System; and
- access to the Brief Enquiry Management System (BEAMS) data via the Justice Warehouse.

OCSAR has agreed to adhere to standards stipulated in the MoU with respect to the security and storage of data, and obtaining relevant ethics committee approval for research and evaluation projects (see separate exemption provided to OCSAR to enable it to collect the required personal information from SAPOL).

This exemption will apply during the period of operation of the MoU, and will cease to apply upon review or invalidation of the MoU. Continued application will be reviewed if the MoU is amended.

Expiry

This exemption will be reviewed by OCSAR, SAPOL and the Privacy Committee five (5) years after approval, or upon review or amendment of the MoU, whichever is sooner. An extension may be negotiated with the Privacy Committee if required.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*. The Privacy Committee may be consulted on the development of disposal authority if required.

(Original signed)

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
10 September 2007

(Approval granted at the meeting 13 June 2007)

Exemption for Office of Crime Statistics and Research

In accordance with Clause 4 of the Privacy Committee's Proclamation the following exemption from *Cabinet Administrative Instruction 1/89 'The Information Privacy Principles'* is granted.

This exemption applies to the Office of Crime Statistics and Research (OCSAR). It is an exemption from compliance with Principles 2 and 8, allowing collection of personal information from South Australia Police (SAPOL), and use of that personal information for the purposes of statistical monitoring, research and evaluation projects. Conditions apply.

All other Principles continue to apply.

Compliance

The Principal Officer of OCSAR must ensure compliance with this exemption.

Conditions

This authorisation for collection and use of personal information is conditional.

The personal information to be disclosed is described in the Memorandum of Understanding (MoU) between OCSAR and SAPOL. A synopsis of the MoU is available upon request. Broadly, it includes:

- extracts from SAPOL of unit record data from the Police Incident Management System;
- access to the SAPOL General Enquiry Information System in the Justice Information System; and
- access to the Brief Enquiry Management System (BEAMS) data via the Justice Warehouse.

The projects for which the personal information may be used must be consistent with the role and functions for which OCSAR was established, and must adhere to standards stipulated in the MoU with respect to the security and storage of data.

Relevant ethics committee approval must be obtained for research and evaluation projects.

This exemption will apply during the period of operation of the MoU, and will cease to apply upon review or invalidation of the MoU. Continued application will be reviewed if the MoU is amended.

The data custodian, SAPOL, is willing and able to provide the data to OCSAR (see separate exemption provided to SAPOL to enable it to disclose the required personal information to OCSAR).

Expiry

This exemption will be reviewed by OCSAR, SAPOL and the Privacy Committee five (5) years after approval, or upon review or amendment of the MoU, whichever is sooner. An extension may be negotiated with the Privacy Committee if required.

Destruction or retention of personal information

Destruction or retention of the personal information must be undertaken in accordance with a disposal authority under the *State Records Act 1997*. The Privacy Committee may be consulted on the development of disposal authority if required.

(Original signed)

Terry Ryan
Presiding Member
PRIVACY COMMITTEE OF SOUTH AUSTRALIA
10 September 2007

(Approval granted at the meeting 13 June 2007)