



Government
of South Australia

Annual Report
2005-2006

Privacy Committee
Of South Australia

Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2006

Annual Report 2005-2006

September 2006

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) 8226 7750

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, 2006

Annual Report 2005-2006

The Hon Michael Wright MP
MINISTER FOR ADMINISTRATIVE SERVICES AND
GOVERNMENT ENTERPRISES

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 2006. 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.

A handwritten signature in black ink, appearing to read 'Terry Ryan', with a stylized, cursive script.

Terry Ryan
PRESIDING MEMBER
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

29 September 2006

Table of Contents

1	Introduction	5
2	South Australian Public Sector Privacy Framework	6
2.1	The Information Privacy Principles	6
2.2	The Privacy Committee of South Australia	6
3	Activities of the Privacy Committee	10
3.1	Advice to the Minister	10
3.2	Developments in other jurisdictions	10
3.3	Exemptions	12
3.4	Recommendations and submissions	16
3.5	Complaints	18
3.6	Communication	18
3.7	Keep informed as to the extent to which the Information Privacy Principles are implemented	20
	Appendix 1: Information Privacy Principles	22
	Appendix 2: Proclamation of the Privacy Committee of South Australia	29
	Appendix 3: Exemption Granted – Office of Crime Statistics and Research.....	33
	Appendix 4: Exemption Granted – Department of Health and Department of Families and Communities	35

1 Introduction

This is a report of the activities of the Privacy Committee of South Australia (the Privacy Committee) for the year ending 30 June 2006. It has been developed pursuant to Clause 3(1) of the Proclamation establishing the Privacy Committee (see Appendix 2).

During this reporting year the most prevalent issues that came before members reflected a shift in government service delivery towards increased use of data sharing. Agencies have been seeking more advice on how they can meet their privacy obligations as they collaborate with other agencies in initiatives that call for information sharing across the traditional departmental boundaries.

Inconsistency of privacy protection across Australia is still a problem. The Privacy Committee looks forward to the report by the Australian Law Reform Commission on its review of the *Privacy Act 1988 (Cth)* (see 3.2.1.1), as well as the New South Wales Law Reform Commission report on its review of laws in that state that impact privacy protection (see 3.2.1.2).

The Privacy Committee continues to be concerned about the need to strengthen the privacy regime in South Australia to one that addresses current and emerging privacy issues. Initial approaches have been made to review South Australia's privacy regime (see item 3.4.2).

The Privacy Committee granted two exemptions (see item 3.3), concluded seven of ten complaints (see item 3.5) and established the Privacy Officer Network (see item 3.6.1).

2 South Australian Public Sector Privacy Framework

2.1 The Information Privacy Principles

South Australia's Information Privacy Principles 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 Information Privacy Principles 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 1 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 are described in this Proclamation. A copy of the Proclamation can be found following the Information Privacy Principles Instruction.

2.2.2 Reporting

The Privacy Committee reports to the Minister for Administrative Services and Government Enterprises, 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.

Annual Report 2005-2006

For this reporting year, the Privacy Committee comprised:

Presiding Member:

- ▶ Terry Ryan, Director, State Records of South Australia, Department for Administrative and Information Services

Members:

- ▶ Anne French, Manager Workforce Strategy, Office of Public Employment (resigned April 2006)
- ▶ Gaby Jaksa, Negotiation Coordinator, Department for Administrative and Information Services
- ▶ Bernadette Quirke, Senior Solicitor, Crown Solicitor's Office, Attorney-General's Department
- ▶ Nancy Rogers, Manager, Research & Analysis, Department for Families and Communities (commenced April 2006)
- ▶ 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

The Privacy Committee does not administer a budget. The Department for Administrative and Information Services through State Records provides resources for the Privacy Committee. This facilitates research, advisory and executive support to the Privacy Committee and a public enquiry service. The resources include the commitment of time from various personnel, forming the equivalent of approximately 1.0 FTE.

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. Fees may not be paid, in general, to Government employees. Therefore 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 eleven occasions, including one workshop. 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 approved 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 consistent with *Government Boards and Committees: Guidelines for Agencies and Board Directors* (Department of Premier and Cabinet, 2000). At the conclusion of the reporting year, the Department of Premier and Cabinet Guidelines were under review in light of recent amendments to the *Public Sector Management Act 1995*.

A copy of the handbook for members is available by contacting State Records of South Australia.

2.2.7 South Australia's Strategic Plan

South Australia's Strategic Plan (the Strategic Plan) calls for performance improvement across the South Australian public sector by improvement in productivity and quick decision-making (South Australia's Strategic Plan Objective 1: Growing Prosperity: Targets T1.18 and T1.19).

Annual Report 2005-2006

The Strategic Plan calls for agencies to ‘collaborate to improve access to services [and] increase ... resource sharing’ (Objective 5: Building Communities: Priority Actions). The Privacy Committee’s observation is that there has been an increase in data matching and sharing activities, which results in a challenge for agencies in adherence to their obligations over personal information.

The Privacy Committee has supported 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 2006’. During the reporting year the Privacy Committee had exactly 50% female membership.

2.2.8 Other reporting requirements of public sector agencies

Regulations under the *Public Sector Management Act 1995* describe the reporting requirement of Public Sector agencies. Please refer to the Annual Reports of State Records of South Australia and the Department for Administrative and Information Services for matters within the scope of Human Resource Management and Financial Management of the office supporting the Privacy Committee.

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, including a proposal for a review of the privacy regime (see item 3.4.2).

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 significant interest to the Privacy Committee. An overview follows of 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

On 31 January 2006, the Australian Law Reform Commission announced that it would review the Commonwealth *Privacy Act 1988* (the Act). The 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 will consider relevant existing Commonwealth, State and Territory laws and practices, constitutional issues and other matters, and is likely to comment on the South

Annual Report 2005-2006

Australian Government's Information Privacy Principles, and on the State's relevant existing and proposed laws and practices, such as the *Listening and Surveillance Devices Act 1972*.

The Privacy Committee has registered interest in being kept informed of the progress of the review. The review is to be completed by 31 March 2008.

3.2.1.2 New South Wales Law Reform Commission Review of New South Wales Acts

On 11 April 2006, it was announced that the New South Wales Law Reform Commission would inquire into whether existing legislation in that State provides an effective framework for the protection of the privacy of an individual. This review will consider the desirability of a consistent legislative approach to privacy in the *Privacy and Personal Information Protection Act 1998*, the *Health Records and Information Privacy Protection Act 2002*, the *State Records Act 1998*, the *Freedom of Information Act 1989* and the *Local Government Act 1993*. These Acts apply to New South Wales State Government Departments and Local Government Authorities and, in some cases, to the private sector. The review will also consider the desirability of privacy protection being uniform across Australia. The Commission intends to liaise with the Australian Law Reform Commission as well as other relevant Commonwealth, State and Territory agencies. The desirability of introducing a statutory tort (civil wrong) of privacy in New South Wales will also be considered.

3.2.1.3 Do Not Call Register

On 30 October 2005, the Federal Department of Communications, Information Technology and the Arts issued a discussion paper regarding the introduction of a *Do Not Call Register*, in response to concerns expressed by the general public about telemarketing. See also item 3.4.3.

3.2.2 Conferences and seminars

Throughout the year, representation of the Privacy Committee was made at various conferences, seminars and forums, including:

- ▶ Asia Pacific Privacy Authorities (APPA), formerly known as Privacy Agencies of New Zealand and Australia plus Hong Kong and Korea (PANZA+), hosted by the Victorian Privacy Commissioner, 18 November 2005

Annual Report 2005-2006

- ▶ Privacy Impact Assessment Seminar, hosted by the Office of the New Zealand Privacy Commissioner, Wellington, New Zealand, 29 March 2006
- ▶ Privacy Issues Forum, hosted by the Office of the New Zealand Privacy Commissioner, Wellington, New Zealand, 30 March 2006
- ▶ Multi-Centre Ethical Review: Options for South Australia, hosted by the South Australian Department of Health, 31 March 2006.

3.2.2.1 Asia Pacific Privacy Authorities

Asia Pacific Privacy Authorities (APPA), formerly known as Privacy Agencies of New Zealand and Australia plus Hong Kong and Korea (PANZA+), is the principal forum for regional privacy authorities to form partnerships and exchange ideas on privacy regulation, new technologies and the management of privacy enquiries and complaints. APPA convenes twice a year with meetings hosted on a rotating basis by the various Privacy Commissioners. The forum discusses issues such as privacy and security, identity management, surveillance, cross-jurisdictional law enforcement in the Pacific Rim, privacy legislation amendments, cryptography and personal data privacy.

Formal APPA membership is limited to Privacy Commissioners and their staff. The Privacy Committee is not a formal member, as it does not occupy the role of a Commissioner.

A representative of the Privacy Committee attends most of the extended meetings, depending on the content of the agenda. During this reporting year, APPA meetings were held on 18 November 2005 in Victoria and 17-18 May 2006 in New South Wales. A representative attended the November 2005 meeting.

3.3 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 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 an individual's right to privacy.

Annual Report 2005-2006

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. Research exemptions are therefore granted on a case-by-case basis.

During this reporting year, the following exemptions were considered.

3.3.1 Office of Crime Statistics and Research: collect, use and disclose personal information for the purposes of two research projects

On 16 November 2005, the Privacy Committee approved an exemption for the Office of Crime Statistics and Research (OCSAR) to collect, use and disclose personal information for the purposes of the research project *Tracking Child Abuse Cases from CYFS notification through to police incident report*. A copy of the exemption is attached at Appendix 3.

On 3 May 2006, the Privacy Committee considered a request for exemption from OCSAR to collect and disclose 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 for exemption asked that personal information about VIP clients could be collected by OCSAR without obtaining the clients' consent. The request stated that the information would have any identities removed before analysis was conducted.

The Privacy Committee determined that the request was not justified because the arguments in the submission that supported the public interest of the program did not outweigh the fact that VIP clients receive a confidentiality undertaking when they enter the program. In addition, the low volume of the sample group meant that it would be practical to seek the consent of the VIPs clients to disclose their personal information to OCSAR. The Privacy Committee agreed to reconsider the exemption should further information be supplied by OCSAR in support of the program.

3.3.2 Department of Health and Department for Families and Communities: use of specified administrative data sets, containing information that may identify individuals, in research analysis within the scope of the *Common Clients Project* – Extension

On 9 March 2004, the Privacy Committee approved an exemption from the Information Privacy Principles Instruction to the then Department of Human Services. The exemption allowed the use of specified data sets, containing information that may identify individuals, in research analysis within the scope of the *Common Clients Project – Stage II*. The exemption contained various conditions agreed to in consultation with the then Strategic Planning and Research Branch. One of the conditions was that the exemption would expire on 31 December 2005.

The Department of Health sought an extension to the exemption, as the project was experiencing delays in data collection and data cleaning processes. The Privacy Committee was also advised that it is now a joint project involving both the Department of Health and Department for Families and Communities. On 24 May 2006, the Privacy Committee approved the extension to 30 June 2007 to both departments. A copy is attached at Appendix 4.

3.3.3 Department of Health and the Department for Families and Communities: to collect and disclose personal information for the Child Protection Framework for the Provision of Services

On 3 May 2006, the Privacy Committee considered a request for exemption from the Department for Families and Communities (DFC) to collect and disclose personal information for activities under the Child Protection Framework. The Privacy Committee concluded that an exemption was not necessary because in the Privacy Committee's assessment the *Children's Protection Act 1993* and the *South Australian Health Commission Act 1976* already allow conditional disclosure of personal information. The IPPs are not intended to prevent information flow required to save lives or reduce serious health risks to individuals. Principle 10 (b) and (c), allows disclosure of personal information "to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person" and as "required or authorised by or under law".

The Privacy Committee agreed to reconsider the exemption should the Department understand there to be a conflict between the law, the IPPs (or *Code of Fair Information Practice*) and the information sharing activities described in the submission.

3.3.4 South Australia Police Department: to disclose personal information under certain circumstances

In January 2006, the South Australia Police Department (SAPOL) proposed amendments to the IPPs which would allow SAPOL to use and release personal information concerning crime prevention and matters of public interest. The proposal was withdrawn because amendments to the IPPs were not considered necessary and SAPOL were instead encouraged to seek advice of the Privacy Committee. SAPOL subsequently made a request for exemption from the IPPs. In the request, SAPOL communicated a need to be able to release personal information in some circumstances to counteract paedophile activity, terrorism, drug overdose risks and absconders from mental health facilities, among others.

On 1 March 2006, the Committee denied the request for exemption because of other legislative instruments in place that govern the release of personal information in each of the required circumstances. It was understood that the *Children's Protection Act 1993* and the *Mental Health Act 1993* each contain authorities for disclosure of information under certain circumstances. The Privacy Committee also advised that crime prevention might be considered part of law enforcement when interpreting the IPPs, and that SAPOL should seek further legal advice on their existing capacity to use and disclose personal information.

The Privacy Committee agreed to reconsider the exemption should SAPOL understand there to be a conflict between the law, the IPPs and the information disclosure activities described in the request.

3.3.5 Forensic Science South Australia

In July 2005, the Privacy Committee considered a request for exemption from Forensic Science South Australia (Forensic Science) to be able to collect infectious diseases test results of cadavers prior to conducting an autopsy. The request was made in the interests of

protecting staff health and safety by determining the protective measures that would be required when conducting an autopsy.

The Privacy Committee concluded that an exemption was not necessary because the information relates to deceased persons and the definition of personal information in the IPPs only covers 'natural persons'. Nevertheless the Privacy Committee acknowledged that the information should still be treated with sensitivity and in consideration of living family and friends of the deceased. The Privacy Committee assessed procedures described by Forensic Science, which, if followed, would not offend privacy nor breach the IPPs.

3.4 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. Some key instances are described below.

3.4.1 Review of the Information Privacy Principles

The Privacy Committee submitted a proposal to the Minister in May 2005 to vary the Information Privacy Principles to recognise the activity of contracting for services. Recommendations made in the proposal included undertaking consultation with the Crown Solicitor's Office and State Procurement Board on proposed amendments to the Information Privacy Principles, along with the development of model Terms and Conditions for contracts for service involving the handling of personal information. The Minister subsequently approved the proposal in principle. Work on the proposal has been underway throughout the reporting year, and continues into the next.

3.4.2 Upgrade of Privacy Regime in South Australia

Further to the proposal mentioned at item 3.4.1, in May 2006 the Privacy Committee made a more general submission to the Minister suggesting how privacy may be strengthened in South Australia. The Privacy Committee recommended the development of a consultation

paper on the issue. The Presiding Member was advised of the Minister's in-principle support for the development of the consultation paper.

3.4.3 Discussion Paper: Introduction of a Do Not Call Register

On 30 October 2005, the Federal Department of Communications, Information Technology and the Arts issued a discussion paper regarding the introduction of a *Do Not Call Register*, in response to concerns expressed by the general public about telemarketing. See also item 3.2.1.3.

On 1 December 2005, the Privacy Committee wrote to the Hon Senator Helen Coonan, Federal Minister for Communications, Information Technology and the Arts, in response to a discussion paper regarding the introduction of a *Do Not Call Register*.

Although the intention of the register is to reduce the intrusion into consumers' lives, in its advice to Senator Coonan, the Privacy Committee noted that there are risks in relation to the ownership, management, maintenance and protection of, and access to, personal information stored in public registers. The Privacy Committee therefore advised that it was hesitant to support the creation of a *Do Not Call Register*.

3.4.4 Street to Home Service

The Central Northern Adelaide Health Service 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 the Committee's approval is not required if information is to be shared to reduce danger to the health or life of an individual. Principle 10(b) of the IPPs allows the sharing of information between the relevant parties if required "to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person". If the information sharing does not fall outside the scope and intent of what is allowed under the Principles or relevant legislation, the matter would be concluded.

Discussions continued with Street to Home Service and the Central Northern Adelaide Health Service at the end of the reporting year.

3.5 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’.

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

Of the seven completed complaints:

- ▶ one involved a breach of the Information Privacy Principles and the matter has been addressed by the agency to the satisfaction of the Privacy Committee
- ▶ in one it was unable to be determined whether or not a breach occurred based on the facts provided
- ▶ one was about confidentiality of government business rather than privacy of personal information
- ▶ one was about use of personal information by a private citizen
- ▶ three involved personal information handling activities allowed under specific legislation.

The information involved fell into the subject areas of finances, interactions with police and courts, land holdings, concession status, contact details and reputation.

3.6 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’.

3.6.1 Privacy Officer Network

This reporting year saw preliminary work by the Privacy Committee for the establishment of a Privacy Officer Network across the State Government agencies. In June 2006, invitations were sent to State Government portfolio Chief Executives seeking participation in the Network, which aims to assist Principal Officers of agencies to fulfil their obligation to comply with the IPPs.

The establishment of a Privacy Officer Network will increase the efficiency of communications about the handling of personal information held by the South Australian Public Sector. In turn this will enable proactive responses to areas of privacy risk, and over time will develop a more robust culture of privacy awareness across the Public Sector. A better understanding of the IPPs will also ensure improved data flows in circumstances permitted by the IPPs.

State Records will coordinate the Network.

3.6.2 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 and the South Australian Identity Security and Management Group (formerly the Public Sector Reform Identity Crime Committee).

3.6.3 Telephone and e-mail enquiries

As part of its role to support the Privacy Committee, State Records of South Australia continues to provide a response service for telephone and e-mail enquiries relating to privacy of personal information in South Australia. There were approximately 220 telephone and e-mail enquiries received during the reporting year, which was an increase of 25% from the previous reporting year.

3.6.4 Presentations and publications

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

Privacy was also the subject of a presentation to the Freedom of Information Officers Forum held on 5 April 2006.

3.7 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’.

3.7.1 Arising issues

The Privacy Committee continued to communicate with agencies about matters such as data matching and sharing, and child protection initiatives. New issues on the Privacy Committee’s agenda during the reporting year included:

- ▶ A National Identity Security Strategy
- ▶ Initiatives of the Social Inclusion Unit
- ▶ Training use of a case tracking database
- ▶ A proposed student truancy scheme
- ▶ A multi-agency approach to domestic violence.

3.7.2 Fines Payment Unit

It was reported in the Annual Report for the year ending 30 June 2002 that the Privacy Committee and the Fines Payment Unit (FPU) of the Courts Administration Authority had agreed upon a set of data matching protocols. The protocols were to be used by the FPU in its use of data from other State Government agencies for the purposes of locating fine defaulters.

Annual Report 2005-2006

One of the conditions of the protocols was that the FPU would report annually to the Privacy Committee on the activity of the data matching program.

Data matching:

- ▶ commenced with the Residential Tenancies Branch of the Office of Consumer and Business Affairs in early 2003 and ceased in December 2003
- ▶ commenced with South Australia Police Department in early 2003 and continues to date. These are the only agencies that have participated in the data matching activity.

Since the implementation of data matching the FPU has not received any complaints regarding the system.

Appendix 1: 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):

Annual Report 2005-2006

‘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

Appendix 2: 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

Annual Report 2005-2006

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.

Appendix 3: Exemption Granted – Office of Crime Statistics and Research

See also item 3.3.1.

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 Office of Crime Statistics and Research (OCSAR), within the Department of Justice, exempting OCSAR personnel from complying with the IPPs to collect, use and disclose personal information for the purposes of the research project *Tracking Child Abuse Cases from CYFS notification through to police incident report*.

The exemption is dependent upon the following conditions:

- ▶ Data linkage within the Office of Crime Statistics and Research (OCSAR) is to be separated from data analysis. That is, the Database Manager is to perform the linkage of the two data sets with a unique identifier assigned to each individual. The linked data set (which will not contain any names, addresses or dates of birth) will then be provided to the researcher for analysis.
- ▶ The approach to be adopted for the management of data provided by agencies to OCSAR has been outlined as follows:
 - ▶ The agency will provide OCSAR with a data dictionary and copy of any counting rules, which have been applied, along with any other caveats around the reliability etc of the data.
 - ▶ The data file provided to OCSAR is to be transferred via tape or disc, which has been encrypted, or via access provisions negotiated with the individual agency. No transfer of data will occur via email unless such data is encrypted and password protected. Passwords for the file are to be provided (separate from the data) to the Database Manager.
 - ▶ As soon as practicable, upon receiving a data file from an agency the Database Manager is to:

Annual Report 2005-2006

- Allocate a unique identifier to each individual (such as the Justice Information System PIN) contained in the data set: and
 - Link the data to an existing OCSAR dataset, which has been prepared for the project.
 - The linked file, which will not contain identifying information provided by the agency, will then be stored in accordance with the data storage protocols within OCSAR.
- ▶ All data reported on by OCSAR is to be de-identified and aggregated, so as not to identify individuals or communities. The data is to be published in a final report made to relevant government stakeholders (eg CYFS executive, SAPOL executive etc). A decision as to whether to release the report more widely is to be made in consultation with these stakeholders.

This exemption will expire five (5) years from approval (16 November 2010), or upon reversal or expiration of Human Research Ethics Committee approval, or upon completion of the research project, whichever is sooner.

Terry Ryan

Presiding Member

PRIVACY COMMITTEE OF SOUTH AUSTRALIA

(Approval granted at the meeting of 16 November 2005)

Appendix 4: Exemption Granted – Department of Health and Department of Families and Communities

See also item 3.3.2.

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 Health (DH) and the Department for Families and Communities (DFC), exempting it from complying with Information Privacy Principle 8 in the conduct of the *Common Clients Project – Stage II*. This is an extension to a previous exemption granted on 9 March 2004 to the then Department of Human Services and therefore applies to the two departments as far as they are involved in the conduct of the project.

It allows the use of specified administrative data sets, containing information that may identify individuals, in research analysis within the scope of the Common Clients Project.

(It is significant that the information is to be depersonalised by coded geographical details being randomly shifted. The Project is outlined further in the Second Report of the project in August 2003 and application to the Human Research Ethics Committee in September 2003).

Any change to the methodology of the Project may require a review of this Exemption.

DH or DFC will inform the Privacy Committee if a breach of any of the above conditions occurs. If the Human Research Ethics Committee reverses its support for the project, the exemption will cease.

The exemption will expire at the conclusion of the Common Clients Project, or on 30 June 2007, whichever is first.

Terry Ryan

Presiding Member

PRIVACY COMMITTEE OF SOUTH AUSTRALIA

(Approval granted at the meeting of 10 April 2006)