



Government
of South Australia

Annual Report

Privacy Committee
Of South Australia

Annual Report of the Privacy Committee of South Australia

For the year ending 30 June 2004

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

Annual Report of the Privacy Committee of South Australia
For the year ending 30 June 2004

Page 1 of 35



Government
of South Australia

Annual Report

September 2004

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, 2004



Government
of South Australia

Annual Report

The Hon. Michael Wright MP
MINISTER FOR ADMINISTRATIVE SERVICES

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 2004. 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'.

Terry Ryan
PRESIDING MEMBER
PRIVACY COMMITTEE OF SOUTH AUSTRALIA

23 September 2004



Table of Contents

1	Introduction	5
2	South Australian Public Sector Privacy Framework.....	7
2.1	The Information Privacy Principles	7
2.2	The Privacy Committee	7
3	Business of the Committee	10
3.1	Advice to the Minister	10
3.2	Keeping Informed of Developments in Other Jurisdictions.....	10
3.3	Exemptions	13
3.4	Recommendations and Submissions.....	15
3.5	Complaints.....	19
3.6	Communication	19
3.7	Compliance.....	20
	Appendix 1: Information Privacy Principles.....	22
	Appendix 2: Proclamation of the Privacy Committee of South Australia ..	28
	Appendix 3: Exemption Granted – Department of Human Services.....	32
	Appendix 4: Exemption Granted – South Australia Police.....	34



1 Introduction

The Privacy Committee of South Australia (the Committee) has enjoyed one of its more productive years in 2003-04, with some significant interactions with a range of public sector agencies. Throughout the year, agencies have been more active in seeking the advice and recommendations of the Committee, and, as a result of a number of complaint cases in the past three years, the Committee has taken the opportunity to improve liaison across a broad range of agencies. There also appears to be a renewed interest in information privacy from within the agencies and this has led to an increase in requests for training and awareness presentations, and consultation on programs and projects which involve the management of personal information.

Key issues, identified throughout this and other years, for both agencies and the public include:

- ▶ identity crime, which may involve identity theft or fraud (see 3.2.2);
- ▶ storage and management of genetic information, eg information that may be found in the Guthrie Test cards (see 3.7.1); and
- ▶ surveillance or covert filming and distribution, eg cameras in mobile phones (see 3.2.3).

More than half of the complaints handled by the Committee during the year were concluded when it was found that the agency had the legislative authority to manage the personal information in the way that it did. This highlighted to the Committee how divergent the views of the public and government are in the way personal information is managed. In some cases, the Committee was able to bring these views to the attention of the agency and recommend a more sensitive practice be considered.



**Government
of South Australia**

Annual Report

The terms of appointment for the members described in this report expired on 25 May 2004 and the formation of a new Committee is underway. The Committee, in conjunction with staff from State Records of South Australia (State Records), plans to review the privacy regime in the coming year and make recommendations to Government for the future management of privacy in South Australia.



2 South Australian Public Sector Privacy Framework

2.1 The Information Privacy Principles

South Australia's Information Privacy Principles (IPPs) were introduced by means of Cabinet Administrative Instruction 1/89 and are more commonly known as the Information Privacy Principles Instruction. The IPPs first became operational in July 1989. The IPPs regulate the way South Australian Public Sector agencies can collect, use, store and disclose personal information. A copy of the IPPs, within Cabinet Administrative Instruction 1/89, can be found on the Department of Premier and Cabinet website at www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf, and in Appendix 1 of this document.

2.2 The Privacy Committee

2.2.1 Constitution

The Privacy Committee of South Australia was established by proclamation in the Government Gazette on 6 July 1989. A copy of the proclamation can be found following the IPPs on the Department of Premier and Cabinet website at www.premcab.sa.gov.au/pdf/circulars/Privacy.pdf, and in Appendix 2 of this document.

2.2.2 Responsibility

The Committee reports to the Minister for Administrative Services, which for 1 July 2003 to 5 March 2004 was the Hon. Jay Weatherill MP, and for 5 March to 30 June 2004 was 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 Human Services; and
- ▶ 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 for Administrative and Information Services.

Members:

- ▶ Andrew Stanley, Director, Strategic Planning and Research Branch, Strategic Planning and Population Health Division, Department of Human Services.
- ▶ Anne French, Principal Consultant, Office for the Commissioner for Public Employment.
- ▶ Gaby Jaksa, Project Director, Department for Administrative and Information Services.
- ▶ Milton Spurling, Non-public sector representative.
- ▶ Maria Panagiotidis, Managing Solicitor, Crown Solicitor's Office, Attorney-General's Department (to August 2003).
- ▶ Dr Nicholas Manetta, Managing Solicitor, Crown Solicitor's Office, Attorney-General's Department (from December 2003).

The terms of appointment of all members expired on 25 May 2004. At 30 June 2004, the Minister was seeking nominations for a new Committee.



2.2.4 Functions

The functions of the Committee are:

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

2.2.5 Resources

The Committee does not administer a budget. The Department for Administrative and Information Services provides resources for the Privacy Committee. This includes research, advisory and executive support to the Committee, which is provided by State Records.

2.2.6 Meetings

The Committee met on nine occasions during the reporting year.



3 Business of the Committee

3.1 Advice to the Minister

The Committee is required, 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 Committee has briefed the Minister on matters relating to privacy, including legislative and administrative action to protect individual privacy, and has provided advice as required during the year. These briefings have built upon advice in previous years proposing the introduction of privacy legislation which would apply, in particular, to the South Australian State and Local Government and University sectors.

3.2 Keeping Informed of Developments in Other Jurisdictions

The Committee is required, under clause 2(a) of the Proclamation, “to keep itself informed of developments in relation to the protection of individual privacy in other jurisdictions”.

Within Australia, the Commonwealth and each State and Territory operate under varying legislative and policy environments for privacy protection. These regimes are of significant interest to the Privacy Committee.

Developments in related areas such as freedom of information are also relevant.



3.2.1 Commonwealth, States and Territories

The Office of the Victorian Privacy Commissioner released a concise and useful overview of existing privacy regulation in Australia, across the Commonwealth, States and Territories, as at 30 June 2004. This publication is viewable at www.privacy.vic.gov.au. The only recent legislative development in Australia was the commencement of the Northern Territory *Information Act 2002*, on 1 July 2003. This Act came into force on 1 July 2004.

The Commonwealth *Privacy Act 1988* applies to the Commonwealth Government and to most private sector organisations. Privacy laws apply to state, territory and local government sectors in the Australian Capital Territory, New South Wales, Victoria and the Northern Territory. Tasmania and Western Australia have indicated an intention to develop privacy legislation. At present, South Australia, Queensland and Tasmania rely on administrative privacy standards to regulate privacy within government.

The Committee is observing the developments in other jurisdictions and, with the assistance of State Records, is developing a paper regarding the future of the privacy regime in South Australia for consideration by the Minister.

Throughout the year, representatives of the Committee attended various conferences, seminars and forums, including:

- ▶ Galleries, Libraries, Archives and Museums (GLAM) Conference, Adelaide, September 2003, and
- ▶ Privacy Agencies of New Zealand and Australia (PANZA+) Meeting, Melbourne, November 2003.



3.2.2 Issues of National Importance: Identity Theft

The phrase ‘identity crime’ is used to describe criminal activity in which a perpetrator uses a false identity in order to commit a crime. Identity crime can underpin a range of crimes including people smuggling, drug trafficking, money laundering, and terrorism. The extent and cost to the community of identity crime is difficult to quantify given this broad range of offending. In 2001, the Commonwealth Attorney-General’s Department estimated the potential cost of identity fraud to be more than \$4 billion annually.¹

A false identity is often gained through ‘identity theft’, in which a perpetrator commandeers the identity of another person (living or dead) by using stolen personal information, or fraudulently obtained, forged, or stolen identity documents.

In July 2004, the Privacy Committee was invited to comment on the *Criminal Law Consolidation (Identity Theft) Amendment Bill 2003*. The Committee commended the Attorney-General on introducing a Bill that recognises the offence of identity theft and recommended that it be approved for introduction to Parliament.

The Committee was invited, in June 2004, to participate in a “Public Sector Reform Working Group for Identity Crime”. The Officer-in-Charge of the Commercial and Electronic Crime Branch of the South Australia Police Department (SAPOL), chairs the working group. It is proposed to develop an Identity Crime State Strategy that will focus on six areas of reform and address issues with implications for information privacy, such as information exchange or data sharing.

¹ Attorney-General’s Department (2001), *Scoping Identity Fraud*. September. Canberra.



3.2.3 Issues of National Importance: Video Surveillance

The Committee continues to maintain interest in the growing use and awareness of video surveillance. Media interest during the year centred on the use of mobile phone cameras to record and transmit images, and especially the potential for violations of privacy when used in facilities such as change rooms.

In the House of Assembly on 24 October 2003, the Hon. Kris Hanna MP proposed to amend the *Listening and Surveillance Devices Act 1972* to include the recording of covert video. By the close of the reporting year no further development had taken place in this regard.

3.3 Exemptions

The 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 Committee thinks fit”.

Requests for exemptions are addressed on a case by case basis. This power is only applied in situations where the public interest outweighs an individual's right to privacy.

All exemptions granted by the Committee since exemptions began in 1990, are currently under review with the intention of retirement, revocation, updating or amendment. Where appropriate, an expiry term may be added to an exemption to allow for periodic review in the future. More than 30 exemptions have been granted by the Committee since 1990, many for one-off research projects that are no longer in progress.



One exemption in particular is under review. It was granted to SAPOL and permitted, with conditions, the disclosure of vehicle collision report details to certain parties to the collision. At the close of the reporting year, the Committee was in discussion with SAPOL regarding the relevance of this exemption and its conditions.

During this reporting year, the following exemptions were sought:

3.3.1 Department of Human Services: Common Client Project

The Department of Human Services (DHS) requested that it be exempted from Principle 8 of the IPPs in order to allow the use in research of specific data containing information that may identify individuals. The data would be used in a particular project assessing resource use by common clients of various DHS businesses.

The project had the endorsement of the DHS Human Research Ethics Committee. The Privacy Committee was satisfied by the methodology of the research and so granted an exemption on 15 March 2004. A copy of the exemption is found in Appendix 3.

3.3.2 South Australia Police: Vehicle Collision Reports

In August 1997, SAPOL was given an exemption allowing them to release vehicle collision report information to the State Government Insurance Commission (SGIC). Release was to be provided to meet SGIC's needs as the compulsory third party insurer at the time. In August 2003, SAPOL submitted a request to update the exemption so it could apply to an information sharing agreement between SAPOL and Allianz. Allianz is the new, approved insurer under contract with the Motor Accident Commission.

An exemption from complying with Principle 10 of the IPPs was granted to SAPOL in October 2003. A copy of this exemption is found in Appendix 4.



3.4 Recommendations and Submissions

The Committee is required, 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 Committee responded to various requests for advice, support and recommendations. Some key instances are described below.

3.4.1 Australian Health Ministers' Advisory Council: National Health Privacy Principles

In the previous reporting year, the Australian Health Ministers' Advisory Council (AHMAC) established a Privacy Working Group to develop and implement a national Privacy Code (the Code) and guidelines. The intention of the Code was to establish a nationally consistent framework for health-related privacy. In May 2003, the then Minister for Administrative Services, the Hon. Jay Weatherill MP, consulted with the Privacy Committee and made a submission to AHMAC that the addition of this privacy protection scheme for health records would not provide any greater protection of privacy for South Australians than the current framework. The framework includes a Code of Fair Information Practice for the Human Services sector that mirrors the National Privacy Principles contained in the private sector provisions of the Commonwealth *Privacy Act 1988*.

In April 2004, the Minister for Health, the Hon. Lea Stevens MP, wrote to the Minister for Administrative Services, the Hon. Michael Wright MP, advising that AHMAC was now considering options for implementation of the proposed Code, and sought advice as to the preferred options.



Minister Wright responded that, from the options provided, he recommended that the proposed Code be adopted as a schedule to the Commonwealth *Privacy Act 1988*, to cover the Australian Government public sector and private sector nationally, and be incorporated into State and Territory public sector privacy arrangements. It was considered that this option provided the greatest continuity across all Australian jurisdictions.

3.4.2 Proposed Amendments to the Controlled Substances Act 1984 and Regulations

In December 2003, DHS consulted the Committee in regard to proposed amendments to the *Controlled Substances Act 1984* and Regulations. The amendments were considered necessary to improve the prevention and investigation of criminal abuse of prescribed medicines and some over-the-counter medicines. The Committee responded with a number of recommendations to be considered to ensure that information collected relating to individuals would not be used or disclosed outside the requirements of the *Controlled Substances Act*.

3.4.3 Office of Consumer and Business Affairs: Publication of Registers on the Internet

The Office of Consumer and Business Affairs (OCBA) has a function to administer several public registers, which are databases of licensed service providers in South Australia and their employees. Each register is established by a piece of legislation governing the licensing of a particular set of service providers, such as a plumber or an electrician. The public nature of the registers is established by each piece of legislation so the information may be used by members of the public to verify the licence status of a service provider. They have also been used by industry training providers to verify the status of their customers. Further, the registers act as locality guides to available services and include, for each service provider, an address for the service of notices.



Following a complaint from a member of the public, the Privacy Committee expressed concern about the OCBA's publication of its registers on the Internet. Of particular concern was the potential for mis-use of the information in the on-line environment, and the inability of a licensee to suppress their address.

While the complaint related to one register, it was noted that any resolution to the problem would apply to all registers under the OCBA's licensing function.

The laws establishing the registers do not always require an address to be publicly listed. As it stood, there was no opportunity for the licensee to suppress their home address from publication or inspection, and so the occasional licensee who did not wish to have their home address published was unable to protect their privacy.

After advice from the Committee, the OCBA made some immediate changes. They removed the addresses of employees of service providers from the registers, as there was no need for their service addresses to be listed. The OCBA also changed their procedures such that all applicants for licence are now informed of where and why information is made available to the public. Various other recommendations are being considered by the OCBA.

3.4.4 Child Protection: National Paedophile Register

One of the recommendations of the *Report of the Review of Child Protection in South Australia*, conducted by Ms Robyn Layton QC, was for the establishment of a register of 'unsuitable persons'. The Committee wrote to the Child Protection Review Secretariat, within DHS, offering to contribute towards the development of the register if the recommendation were to be implemented. In its capacity, the Committee would be able to provide advice around the scope of the register and how the information might be used.



In a separate scheme, the Hon. Kevin Foley MP, the Police Minister, agreed to South Australia joining the Australian National Child Offender Register. The Committee consulted SAPOL and found that the proposed national register is based on a CrimTrac (Federal) proposal and a New South Wales model. The Victorian Department of Justice has drafted a central legislative model from which the Commonwealth and States and Territories have agreed to draft its own legislation.

A national register would contain information about individuals convicted of crimes such as the murder of a child or committing, or conspiring to commit, a range of sexual offences against children. The offender must supply their name, date of birth, address and the names and ages of any children who generally reside with them. They must also provide details of their employment, car, distinguishing marks or tattoos, affiliation with any club that has child members and convictions of registrable offences in foreign jurisdictions.

As it stands, SAPOL is not currently prevented from maintaining a register for intelligence purposes, provided it meets the criteria of the Information Privacy Principles. The central difference with a national register is that of information sharing across jurisdictions, or disclosure to third parties.

While South Australian legislation has not yet been developed, the Committee will be invited to participate in the development of protocols and guidelines around its implementation.



3.5 Complaints

The Committee is required, 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”.

During the reporting year, the Committee handled complaints from fifteen individuals alleging violations of their privacy. Communication with five of these complainants was carried over from 2002-03, and one from 2001-02.

Two complaints were still under consideration at year’s end. Of the thirteen completed complaints, eight were concluded when it was determined that legislation gave the agency the authority to perform the operations which were the subject of the complaint. Of the five remaining complaints two were referred to the Federal Privacy Commissioner, one was referred to a University and two were advised that their complaints did not relate to information privacy.

3.6 Communication

The Committee is required, 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 Participation in Committees and Groups

The Committee is represented on the DHS Departmental Ethics and Privacy Committee and the Justice Information Systems Privacy Committee. The Committee was also represented at the meeting of the Privacy Agencies of New Zealand and Australia (PANZA+) in Melbourne in November 2003.



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

3.6.2 Telephone Enquiries

The Committee receives occasional reports in relation to a telephone enquiry service provided by State Records on privacy issues. The reports are statistical in nature and no personal details of callers are retained.

During the reporting year, there was a dramatic reduction in the number of telephone enquiries handled by State Records. This has been attributed, in part, to an arrangement in which Service SA responds to the first line of enquiries about various State Records services, including privacy. Further to this, entries for 'privacy' in the telephone directory were amended to guide callers to the most relevant privacy agency, such as the Office of the Federal Privacy Commissioner, where the issue was not related to South Australian Public Sector business.

3.6.3 Presentations and Publications

During the year, a representative of the Committee gave several presentations of an IPP awareness session, and consideration will be given to formalising such sessions into a future training program.

The new State Records website, launched in April 2004, includes a significant improvement in the quality and quantity of information available regarding privacy.

3.7 Compliance

The Committee is required, 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 Newborn Screening Cards

In the previous reporting year, the Committee reported that they had sought information from the DHS about the collection, storage and use of Guthrie Test Cards in South Australia.

The Guthrie Test is a newborn screening test to detect congenital metabolic disorders, which has been undertaken in South Australia since 1962. During the test, blood is collected from the newborn and spotted onto filter paper and then dried. The information recorded on the card includes details about the child, mother, hospital and referring doctor. The testing is undertaken by the Department of Chemical Pathology at the Women's and Children's Hospital.

Following the inquiry into the protection of human genetic information by the Australian Law Reform Commission and the Australian Health Ethics Committee, DHS began a review into its procedures for handling and retaining the Guthrie Test Cards. In November 2003 the Guthrie Test Cards Review Working Party was established, and included a representative of the State Records Council. Some of the options being considered by the working party include the limited retention of identified cards, and the ongoing retention of de-identified cards for research purposes.

The Committee has a strong interest in the protection of the privacy of the genetic information stored within the blood samples on the Guthrie Test Cards.



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):
"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 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 – Department of Human Services

Note: The *Code of Fair Information Practice*, approved by the Privacy Committee for use within the Department of Human Services, 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.

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 applies to the Department of Human Services (DHS), exempting it from complying with Principle 8 in the conduct of the Common Clients Project – Stage II. 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 DHS Human Research Ethics Committee in September 2003.)

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

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



**Government
of South Australia**

Annual Report

The exemption will expire at the conclusion of the Common Clients Project, or on 31 December 2005, whichever is first.

Terry Ryan

Presiding Member

PRIVACY COMMITTEE OF SOUTH AUSTRALIA

15 March 2004



Appendix 4: Exemption Granted – 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 applies to the South Australia Police (SAPOL), exempting them from complying with Principle 10 (~~see Attachment 1~~). It allows the release of Vehicle Collision Report (VCR) information to Allianz, in its capacity as an approved insurer of the Motor Accident Commissioner (MAC), when the following conditions are met:

- ▶ the information is about collisions resulting in death or bodily injury (as defined in Part 4 of the *Motor Vehicles Act 1959*);
- ▶ the information is used only for the purpose of compulsory third party insurance business (also as defined in Part 4 of the *Motor Vehicles Act*) and is not available to other sections of Allianz;
- ▶ the information may contain blood alcohol content test results providing the result is over 0.05 and is for the driver of a vehicle involved in a collision resulting in death or bodily injury (as above); and
- ▶ auditable security measures are in place to monitor that access to the information is restricted to these conditions.

Other related information may only be released with the consent of the record subject. IPP 10 will continue to apply outside of the conditions of this or any other exemption.

SAPOL will inform the Privacy Committee if a breach of any of the above conditions occurs.



The exemption will expire at or before expiration or termination of the contract between the Motor Accident Commission and Allianz ("MAC Agreement"), or the agreement between the Minister for Police and Allianz for the supply of data by SAPOL to Allianz ("SAPOL Agreement"), whichever is first.

A review of the exemption will take place either 6 months prior to its expiry, or upon relevant amendment or review of the Information Privacy Principles, or at termination of the SAPOL Agreement if less than 6 months notice is given. At the time of approval of this exemption, the MAC Agreement expires on 31 December 2008, and the SAPOL Agreement (in draft at approval of this exemption) expires 3 years after its commencement date.

Terry Ryan

Presiding Member

PRIVACY COMMITTEE OF SOUTH AUSTRALIA

29 October 2003