

CONFIDENTIAL

CABINET DECISION

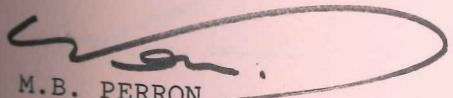
No...6535.....

Submission No.: 5601

Title: PROTECTION OF PERSONAL INFORMATION (INFORMATION
PRIVACY)

Cabinet -

- (a) noted the options paper on the Protection of Personal Information (Information Privacy);
- (b) approved in principle -
 - (i) the establishment of a Committee comprised of representatives from the Department of Law (Chair), Department of the Chief Minister, Department of Lands and Housing, Department of Transport and Works, Conservation Commission, Department of Health and Community Services, Department of Education and the Northern Territory Local Government Association;
 - (ii) the preparation of Administrative Instructions applicable to Territory Departments and Agencies on the lines of the current arrangements operating in South Australia;
 - (iii) that the operation of the Administrative Instructions be reviewed after a period of two years from their commencement, with a view to determining the appropriateness of introducing Territory legislation; and
- (c) directed that -
 - (i) as a first step in the preparation of the Administrative Instructions, an audit be conducted of current practices employed by all Territory departments and agencies in relation to protecting personal information;


M.B. PERRON
Chief Minister

.../2

5 July 1990

CONFIDENTIAL
CABINET DECISION

No...6535.....

2.

Submission No.: 5601

Title: PROTECTION OF PERSONAL INFORMATION (INFORMATION
PRIVACY)

(ii) the result of the audit and consequent recommendations should be referred back to Cabinet within six months of the date of approval to conduct the audit;

(iii) the Department of Law should have carriage of this task.



M.B. PERRON
Chief Minister

5 July 1990

CONFIDENTIAL

CONFIDENTIAL

FOR CABINET

SUBMISSION No:5601.....

Title:	Protection of Personal Information (Information Privacy)
Minister	Chief Minister
Purpose:	Introduce the topic to Cabinet and recommend the preparation a further more detailed report in six months
Relation to existing policy:	Consistent
Timing/ legislative priority:	Normal
Announcement of decision, tabling, etc:	A press release would be appropriate if the Submission is supported
Action re- quired before announcement:	N/A
Staffing implications, numbers and costs, etc:	N/A
Total cost:	N/A

CONFIDENTIAL

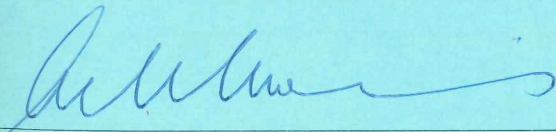
Department/Authority..... **CO-ORDINATION COMMITTEE**

COMMENT ON CABINET SUBMISSION No.

TITLE: PRIVACY LEGISLATION

COMMENTS:

The Committee supports the Submission.



SIGNED:

A.G. MORRIS
Chairman

DESIGNATION:

DATE:

6.6.90

CONFIDENTIAL

CONFIDENTIAL

1

RECOMMENDATIONS

1. It is recommended that Cabinet note the attached options paper on the Protection of Personal Information (Information Privacy) and approve in principle:

- (a) both the establishment of a Committee for the Protection of Personal Information and the preparation of Administrative Instructions applicable to Territory Departments and agencies on the lines of the current arrangements operating in South Australia;
- (b) that the operation of the Administrative Instructions be reviewed after a period of two years from their commencement, with a view to determining the appropriateness of introducing Territory legislation.

2. Provided that Recommendations (a) and (b) are approved by Cabinet, it is further recommended that Cabinet direct:

- (c) that as a first step in the preparation of the Administrative Instructions, an audit be conducted of current practices employed by all Territory departments and agencies in relation to protecting personal information;
- (d) the result of the audit and consequent recommendations should be referred back to

CONFIDENTIAL

CONFIDENTIAL

2

Cabinet within six months of the date of approval to conduct the audit;

- (e) the Department of the Chief Minister should have carriage of this task.

BACKGROUND

3. An interdepartmental committee on privacy legislation was established in February 1990, composed of the Deputy Secretary, Department of Chief Minister (Chair), Secretary Department of Law, and the Deputy Secretary Department of Labour and Administrative Services. The Committee has prepared the Options Paper at Attachment A.

CONSIDERATION OF THE ISSUES

4. Privacy is not a singular, coherent concept. Rather it consists of a range of interests or rights. It seems that for this reason, there has been a reluctance on the part of the legal profession to attempt to create a general tort to protect privacy. Privacy must therefore be examined in its individual parts.

5. There are four broad types of privacy: privacy of the person, territorial privacy, communications/surveillance privacy and information privacy. It is a specific aspect of the latter which has become of increasing concern.

CONFIDENTIAL

CONFIDENTIAL

3

6. An invasion of information privacy includes:
(a) defamation, (b) publication of personal information, (c) breach of confidence, and (d) the inadequate protection of personal information. What distinguishes (a), (b) and (c) from (d) is that the first three are concerned with balancing the protection of personal information interest (or right) against the right of freedom of expression, whilst (d) is concerned with balancing the protection of personal information interest against the interest of governments, businesses and research institutions to use personal information in the effective and efficient operation of their affairs.

7. The need to protect personal information has become of increasing concern world-wide, especially over the last twenty years, with the rapid expansion in information technology, an increase in governmental powers, new and more aggressive business activities as well as increase in research using personal information. With regards to information technology, of particular concern is the linkage of information from different data banks, the centralisation of data banks and information flows across borders.

8. The need to protect personal information need not only rely on "Big Brother" type intrusions, it can be justified on the grounds of human rights and simply good organisational housekeeping.

9. As was noted in paragraph 4, privacy is not a singular, coherent concept. In Queensland and NSW the privacy Acts go beyond dealing with the protection of personal information and cover some of the other types of

CONFIDENTIAL

CONFIDENTIAL

4

privacy. This makes it very difficult in defining rights and responsibilities. There is too much room for ambiguity when one tries to cover entirely different interests or rights.

10. In contrast, the Commonwealth Privacy Act 1988 and the South Australian Cabinet Administrative Instructions (Dec 1988) are only concerned with the protection of personal information. The essence of both of these instruments is a set of eleven Information Privacy Principles (IPPs) which apply to their respective public sector agencies. The two sets of IPPs are almost identical (see Attachment B for the SA IPPs).

11. The IPPs are concerned with the collection, storage, access, correction, use and disclosure of personal information, no matter what the medium of storage (e.g. paper, electronic, audio, photographs, etc.). Principles 5 and 6 are worthy of special attention because they are at the centre of the confusion between Freedom of Information (FOI) legislation and Information Privacy.

12. FOI gives the public a general right to access information held by government. There are, of course, certain types of documents which are "exempt" from access (e.g. Cabinet documents and those relating to law enforcement). There are also exempt agencies (e.g. those in competition with private enterprise).

13. FOI permits access to both personal and general information. No reason needs to be given for seeking access. Experience in Australia has shown that the majority of FOI requests are for personal information.

CONFIDENTIAL

CONFIDENTIAL

5

The government agencies to whom most FOI requests are made for personal information are the service agencies. In the State jurisdictions, typically they include police, health, education, housing, superannuation and correctional services.

14. It was argued in the FOI Options Paper that the right to access one's personal information (SA Principle 5) and the right of an individual to correct his/her own personal information (SA Principle 6) are an integral part of all the other aspects of Information Privacy, namely that only relevant personal information is collected and that this be stored, used and disclosed correctly. FOI does not concern itself with these aspects (i.e. the other nine IPPs).

15. Therefore, it is sensible that FOI should only deal with the right to access non-personal information held by government. In the State jurisdictions, the typical areas of government affected by FOI requests for non-personal information include planning, housing, health, pollution (conservation), transport, education and local government.

16. At present, only the Commonwealth jurisdictions has both FOI and Information Privacy legislation. The available evidence indicates that it favours having the rights to access and correct personal information in the one legislative instrument, namely the Commonwealth Privacy Act 1988.

17. Both the Commonwealth Privacy Act and the SA Cabinet Administrative Instructions specify certain documents and agencies which are exempt from access. The exemptions are similar to those specified in the FOI legislation.

CONFIDENTIAL

CONFIDENTIAL

6

OPTIONS

18. Seven options are discussed within the Options Paper ranging from a do-nothing option on one extreme to the immediate introduction of legislation covering both the public and the private sectors, managed by a Privacy Commissioner, on the other extreme.

19. The preferred option envisages an administrative approach, at least initially. This approach does not preclude the introduction of legislation at a later stage.

PUBLIC IMPACT

20. Any steps taken by Government for the protection of personal information is likely to be welcomed by the public at large. Any disquiet on the part of the government and business sectors is likely to be eased by the gradualist approach recommended. The preferred option places emphasis on education and preventative measures.

FINANCIAL CONSIDERATION

21. Cost of audit would be negligible. If accepted, the first year of operation of the Administrative Instructions is estimated at \$100,000. The estimated expenditure is based on South Australian 1990 expenditure estimates which include one project officer, part-time secretarial support, education and publicity expenses.

CONFIDENTIAL

CONFIDENTIAL

7

COMMONWEALTH/STATE RELATIONS

22. The Administrative Instructions on the Protection of Personal Information would complement existing Instructions and legislation operating in other Australian jurisdictions.

CO-ORDINATION AND CONSULTATION

23. The Submission is a joint product of the Departments of the Chief Minister, Labour and Administrative Services and Law. A comment from the Co-ordination Committee is attached.

PUBLICITY

24. A press release would be appropriate if the Submission is supported.

TIMING

25. No particular timing requirement.

MARSHALL PERRON

CONFIDENTIAL

ATTACHMENT "A"

PROTECTION OF PERSONAL INFORMATION (INFORMATION PRIVACY)

OPTIONS PAPER

1. **DEFINING THE PROBLEM**

Privacy is not a singular, coherent concept. Rather, it consists of a range of interests. It seems that for this reason, there has been a reluctance on the part of the legal profession to attempt to create a general tort to protect privacy and to, in fact, define privacy.

Privacy interests may be grouped into four broad types:

- (a) privacy of the person (an invasion of which includes assault, taking blood samples, body searches, intimidation and harassment);
- (b) territorial privacy (invasion of which is trespass on private property);
- (c) communications and surveillance privacy (an invasion of which includes interception of post or telephone communications, listening devices, "junk" mail and direct marketing by mail or telephone); and
- (d) information privacy (an invasion of which includes defamation, publication of personal information, breach of confidence and the inadequate protection of personal information).

The latter of this group is the subject of this paper.

The above divisions are to assist comprehension and define the problem. It is readily acknowledged that there is some overlap both between and within privacy types. For example, there is an overlap between (a)

and (d), in that taking blood samples to test for drugs or communicable diseases forms the basis of personal information. Similarly, there is an overlap of types (c) and (d). Direct marketing being unsolicited, but person-specific mail or telephone calls, relies on personal information contained in a database which in turn may have been developed from a variety of databases. In contrast to direct mail marketing, "junk" mail is not person-specific and therefore does not rely on a database (the advertising pamphlets are simply distributed to households).

Regarding the overlap within privacy type (d), it can be seen that the first three sub-types, namely defamation, unwanted or unauthorised publicity and breach of confidence may themselves overlap and may also have arisen from the fourth sub-type, namely the inadequate protection of personal information.

What distinguishes the first three information privacy sub-types from the fourth is that the former are concerned with the protection of personal information interest versus the right of freedom of expression; whereas the latter is concerned with the protection of personal information versus the interests of governments, business and research. That is, the former in dealing with freedom of expression tends to be conceptual in nature. The latter is operational in character, being concerned with the conduct of protecting personal information, more specifically, being concerned with governments, businesses and research institutions collecting, storing, using and disseminating personal information.

For these reasons, the term "protection of personal information" is preferred to "information privacy." The preferred term also makes it clear that the information is about an individual person, not for example about a trade secret, as is often the case in breaches of confidence. The word "information" is also preferred to the word "data" (used in the relevant British statute). Although the two words are often used synonymously, "data" consists of symbols which need to be transformed into "information" to be able to be understood. We are here concerned with meaningful data, that is, information.

Personal information may simply be defined as:

"information or an opinion, whether true or not, relating to a natural person whose identity is

apparent, or can reasonably be ascertained, from the information or opinion." (SA Handbook on Information Privacy Principles and Access to Personal Records, p. 5).

2. PROOF THAT THE PROBLEM EXISTS

So far the topic of interest has been narrowed. It is now necessary to demonstrate that in fact a problem or need exists. Two approaches present themselves. First, if sufficient individuals complain about inadequate controls over their personal information, then the establishment of some response mechanism may be justified. In the Northern Territory, for the first quarter of 1990, twenty-two general privacy enquiries were received by the Darwin office of the Commonwealth Human Rights and Equal Opportunity Commission (HREOC). Of these twenty-two enquiries, most were made by individuals and fifteen could have taken action under the Commonwealth Privacy Act 1988. That is, fifteen complaints related to either:

- (a) an alleged breach of principles relating to the protection of personal information by a Federal Department or agency; or
- (b) a breach of Tax File Number security and confidentiality guidelines by a private or public sector employer.

Using these "complaints" statistics as a basis for demonstrating a need has limited validity for at least three reasons. First, despite believing that a breach has been committed, for a variety of reasons some persons may not register their complaint. Second, the Privacy Unit within the Darwin HREOC office is not likely to be well known having been operating for only about one year. Finally, and probably most importantly, an individual often is not aware that an infringement has in fact occurred.

The second approach in demonstrating the existence of a problem or need is the one generally adopted in the information privacy literature, namely that especially over the last twenty years, there has been a rapid expansion in information technology, an increase in governmental powers, new and more aggressive business

activities as well as an increase in research using personal information. However, the need to protect personal information need not only rely on these apparently negative "Big Brother" type intrusions, it can be justified on the more positive grounds of human rights and simply good organisational housekeeping.

Acknowledging that a problem exists in the area of personal information protection in no way implies that all the other privacy issues have been adequately resolved either in the Territory or other Australian jurisdictions. What is being asserted is that the problem of protecting personal information:

- (a) can be clearly identified;
- (b) involves the balancing of competing interests (protection of personal information versus the need of a modern private and public sector to provide a vast range of goods and services efficiently);
- (c) is likely to increase over time (especially during stringent economic periods when calls for efficiency often overshadow individual interests); and
- (d) is essentially practical rather than conceptual in nature and unless other areas of privacy are included in the analysis, the word "interest" is preferred to "rights" and the word "privacy" is better omitted altogether to avoid confusion (in fact, the British Data Protection Act makes no mention of "privacy").

3. THE EXPERIENCE OF OTHER AUSTRALIAN JURISDICTIONS

Privacy legislation exists in Queensland, New South Wales and the Commonwealth. The Commonwealth legislation also covers the Australian Capital Territory. However, the ACT is currently reviewing the situation. South Australia has adopted an administrative approach.

Queensland

In Queensland a part-time Privacy Committee of seven members operates under the Privacy Committee Act 1984. The Committee has no permanent staff working for it and consequently, its profile and activities have been low-key with only one or two complaints being handled per month. The Act has a "sunset clause", which terminates the operation of the Act in August 1990. At present, it is not known what instruments and mechanisms, if any, will replace the current Act and Committee.

New South Wales

New South Wales was the first jurisdiction in Australia to legislate for the "privacy of persons" in the Privacy Committee Act 1975. The statutory Committee has very broad community representation, having a membership between twelve and fifteen. The Committee is independent of government and acts as a privacy ombudsman essentially in an advisory, investigatory and policy-making role. The Committee is serviced by a full-time staff of between three and four people.

The New South Wales Privacy Committee is responsible for a wide range of privacy issues in both the private and public sectors. Although the Committee's major emphasis in recent years has been on the protection of personal information, its concerns extend to any "privacy of persons" matters, such as drug testing, direct marketing, electronic surveillance, credit reporting, and the use of identifying publicity in adoption and fostering.

At present the Committee deals with between 2,000 and 3,000 complaints each year. These high complaints statistics indicate that over the past fifteen years the Committee's services have become well known. However, many of the complaints are of the same type each year ("the individual faces change but not the problems"). This suggests that the privacy brief is too broad and that combined with its limited resources, the Committee not surprisingly tends to be reactive rather than pro-active. The likely result being that the "spot fires" (complaints) will continue to increase without resolving the root cause. Thus, a case can always be made that more staff are required

- 6 -

for an ever increasing number of complaints. Arguably, the solution to the problem is in having a narrower privacy brief and an educative/preventative, rather than a reactive approach. Both the Commonwealth and South Australia appear to meet these two criteria.

The Commonwealth

The Commonwealth Privacy Act 1988 has two major objectives. First, to protect personal information collected by Federal Government departments and agencies. Second, to ensure Tax File Numbers are collected and used only for tax related purposes. The means to achieve these objectives is through the independence, powers and functions of the Federal Privacy Commissioner (supported by a Privacy Advisory Committee).

With regard to the first objective, the Act requires Federal departments and agencies to comply with eleven Information Privacy Principles (IPPs) which govern: the collection, storage and security of personal information; the access by individuals to their own personal records; the accuracy of records; and the use and disclosure of personal information to third parties. That is, the IPPs cover, but only cover, the protection of personal information as previously defined.

The Federal Privacy Commissioner has the authority to ensure agencies comply with the eleven IPPs. The Commissioner can also investigate complaints and award compensation if damages result from any breach of the IPPs. The Commissioner does not have any authority over the private sector except to encourage the voluntary adoption of the IPPs.

The Commissioner's authority may, however, extend to include at least part of the private sector, consumer credit reporting agencies, if the Privacy Amendment Bill 1989 is enacted. The reason that stricter controls are being sought for this industry is that Australia's largest consumer (as against commercial) credit reporting agency, the Credit Reference Association of Australia (CRAA), had signalled its intention to move from "negative" to "positive" or "profile" reporting. Negative reporting refers to information on bad debts, defaults, clearouts and

other repayment problems. Positive reporting refers to current financial commitments and payment history, irrespective of whether or not the individual has ever defaulted.

The CRAA case is a reminder that the Commonwealth has the power to make laws in respect of some important areas, including banking, insurance, interstate trade and commerce, posts, telegraphs and the external affairs power. These are important, given the ability of vast amounts of data to be rapidly transferred across national and international boundaries. However, the States and Territories have the power to make laws in respect of their own government departments and agencies and in respect of most types of businesses operating within their jurisdictions. For the protection of personal information to be meaningful, it should be available to all persons living in Australia, irrespective of where they live, for whom they work and the type of medium (automated or manual) in which various parts of their personal information is stored. To ensure this uniformity of protection for all Australians it is essential that, as a minimum, principles that govern personal information be adopted and that they are similar for all the States, Territories and the Commonwealth.

In the first year of operation, the Federal Privacy Commissioner has concentrated on developing and distributing training packages to ensure departments and agencies understand and comply with the Information Privacy Principles. The goal being to instil knowledge, create an awareness of the issues involved and develop appropriate attitudes and behaviours such that an organisational culture sensitive to the protection of personal information is developed and maintained. Needless to say with this emphasis on "prevention rather than cure", formal complaints constituted a minor part of the Commissioner's workload. For the second year of operation, attention will be focused on the auditing function to ensure compliance with the IPPs and Tax File Number Guidelines.

Given the objectives of the Act and educational approach of the Commissioner, it is not surprising that the Office is expensive to operate. The annual budget of approximately \$1.9m is required for a full-time staff of twenty, office accommodation in Sydney and approximately \$400,000 allocated for consultants and publicity.

South Australia

Although on a smaller scale and at a much lower cost, South Australia's approach is also educational. The SA IPPs and definition of personal information are also similar to that of the Commonwealth. However, whereas in the Commonwealth jurisdiction the instrument used to protect personal information is an Act, in SA it is a Cabinet Administrative Instruction entitled "Information Privacy Principles Instruction" (issued 19 December, 1988). Although the Instrument is a Cabinet instruction, it does not have the force of law, as does an Act.

The second major difference is that the SA Instructions do not provide for an independent, well-resourced Commissioner with wide-ranging powers. Rather, the vehicle for ensuring that the IPPs are being implemented is a Privacy Committee with an administrative support unit comprised of a full-time Project Officer and a part-time typist. The permanent part-time Committee was established in July 1989 and has a membership of four. Two of the members are appointed by the Attorney-General, one by the Government Management Board and one by the Commissioner for Public Employment. Given the appointment procedure, it is not surprising that all four initial members were SA Public Servants. There is some justification for this bias: the Administrative Instructions only apply to the SA Government Departments and agencies (with the exception of the SA Police Department which is governed by virtually identical General Orders). Nevertheless, some compulsory consumer group representation on the Committee would seem appropriate.

The third major difference between the Commonwealth and SA model is that in the latter, written complaints received by the Privacy Committee are referred to "the appropriate authority" with the final authority being the State's Ombudsman, whose powers are more limited than those of the Commonwealth Privacy Commissioner. For example, the latter can award compensation for damages, the Ombudsman cannot.

With respect to the SA Police Department, the final appeal authority is the Police Complaints Authority.

A final major difference between the SA and Commonwealth model is that the SA Privacy Committee must "keep itself informed" in relation to the degree to which the Administrative Instructions are being implemented. The Commonwealth Privacy Commissioner has the power to inspect documents held by Commonwealth Government departments and agencies. This power is extremely important because it ensures that the auditing function can be conducted effectively which in turn is necessary in ensuring that the IPPs have been properly implemented.

4. CHOOSING THE MOST APPROPRIATE RESPONSE

The three variables in examining the options are the instrument, the coverage and the process. The instrument may either be an Act or Cabinet Administrative Instructions. The instrument's coverage may be public sector only or public and private sectors combined. The process, or the mechanism through which the intent of the instrument is to be executed may take two broad forms:

- a Privacy Commissioner Office (possibly supported by an advisory committee); or
- a permanent part-time Privacy Committee with an administrative unit attached.

The available options are presented in tabular form below:

OPTION	VARIABLES		
	INSTRUMENT	COVERAGE	PROCESS
(a)	Nil	Nil	Nil
(b)	Admin Instruct	Public Sector	Committee & Admin Unit
(c)	Act	Public Sector	C'wealth Priv Commissioner
(d)	Act	Public Sector	Committee & Admin Unit
(e)	Act	Public Sector	NT Priv Commissioner
(f)	Act	Public & Priv Sector	Committee & Admin Unit
(g)	Act	Public & Priv Sector	NT Priv Commissioner

Option (a), doing nothing, is not an effective response even if it is argued that the protection of personal information is only a potential problem.

Option (b), in practical terms, is likely to be the quickest to implement and the most flexible to operate and alter because it is not legislative in nature. this option, more than any other, allows for experimentation: to get one's own house (the public sector) in order first before moving into the private sector and more permanent instruments such as Acts.

- 11-

Option (b) is that operating in South Australia. However, improvements on that model can be made, including a broader based Committee membership and clear auditing and compliance powers.

In option (c), Territory legislation would mirror that of the Commonwealth and the Privacy Commissioner would be the Commonwealth Privacy Commissioner who delegates his power to either the Ombudsman or the Territory branch of the Commonwealth, Human Rights and Equal Opportunity Commission (HREOC). It should be noted, however, that the Commonwealth Privacy Commissioner cannot delegate his power to decide cases.

Options (c) to (g) are all legislative in nature. Of these, option (c) is likely to be the simplest to implement. It is also likely to be cheaper than options (e) and (g) which involve the establishment and maintenance of a Territory Privacy Commissioner Office.

There are two reasons why a Commissioner's Office is considered to be more expensive to establish and operate than a Privacy committee supported by an administrative unit. First, a Privacy Commissioner has a higher status and usually a higher public profile. Second, and more significant in terms of costs, the Office of a Privacy Commissioner would probably require more staff than an administrative unit because, as in the case of NSW and SA, some of the workload is undertaken by the Privacy Committee. However, it may be argued that a Privacy Commissioner by tending to have a high public profile and by being perceived by the public as an "identifiable" and powerful person or office, may as a consequence be more effective than a "vague" Privacy Committee.

Except for the fact that option (d) has a legislative instrument, it is identical to option (b). Therefore, the only difference between the two options is that (d) tends to be less flexible, but it does have the force of law.

Of the options covering the public sector only, options (b) to (e), option (e) is likely to be the most expensive as it involves the establishment of a Territory Privacy Commissioner Office.

Of all the options, (f) and (g) are the most comprehensive because they cover both the public and private sectors. Consequently, they are likely to be the most complex and to require more resources to implement and maintain, especially option (g) which incorporates a Commissioner.

There is no philosophical objection to options (c) to (g), only those practical objections or simply drawbacks outlined above. Option (b) is preferred for its simplicity, low cost and particularly its open-endedness with regards to future options.

4. NEXT STEP

If option (b) was accepted, then it would probably be most useful for the relevant Territory department to conduct an audit of current practices employed by all Territory departments and agencies in relation to protecting personal information.

Surveying existing standards is important in (a) determining the current status of protection practices; (b) identifying and assessing the personal information processing needs of each department/agency; and (c) classifying data into different categories of sensitivity. Highest sensitivity data requiring most attention.

THE SOUTH AUSTRALIAN
INFORMATION PRIVACY PRINCIPLES

Principles

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 not be 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. An 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.

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.

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 of the information for that other purpose is necessary or desirable for medical, epidemiological, criminological, statistical or any other genuine research application that is being conducted in a manner that is consistent with authenticated research guidelines;
- (d) the use is required by or under law; or
- (e) the use for that other purpose is reasonably necessary for 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 of the information to that other person is necessary or desirable for medical,

epidemiological, criminological, statistical or any other genuine research application that is being conducted in a manner that is consistent with authenticated research guidelines;

- (d) the disclosure is required or authorised by or under law; or
- (e) 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 or an employer.

Maintenance of Anonymity in Research

11. A researcher should take reasonable steps to ensure that in any product of his or her research the identity of a record-subject, in respect of whose records of personal information he or she has had access, is not disclosed and cannot be ascertained.