LEGISLATIVE ASSEMBLY OF QUEENSLAND

LEGAL, CONSTITUTIONAL AND ADMINISTRATIVE REVIEW COMMITTEE

PRIVACY IN QUEENSLAND

REPORT NO. 9

LEGAL, CONSTITUTIONAL AND ADMINISTRATIVE REVIEW COMMITTEE

	REPORTS	DATE TABLED
1.	Annual Report for 1995-96	8 August 1996
2.	Matters pertaining to the Electoral Commission of Queensland	8 August 1996
3.	The Referendums Bill 1996	14 November 1996
4.	Truth in political advertising	3 December 1996
5.	The Electoral Amendment Bill 1996	20 March 1997
6.	Report on the study tour relating to the preservation and enhancement of individuals' rights and freedoms and to privacy (31 March 1997 - 14 April 1997)	1 October 1997
7.	Annual Report for 1996-97	30 October 1997
8.	The Criminal Law (Sex Offenders Reporting) Bill 1997	25 February 1998

	ISSUES PAPERS	DATE TABLED
1.	Truth in political advertising	11 July 1996
2.	Privacy in Queensland	4 June 1997
3.	The preservation and enhancement of individuals' rights and freedoms: Should Queensland adopt a bill of rights?	1 October 1997

	INFORMATION PAPERS	DATE TABLED
1.	Upper Houses	27 November 1997

LEGAL, CONSTITUTIONAL AND ADMINISTRATIVE COMMITTEE

48TH PARLIAMENT
SECOND SESSION

CHAIRMAN:	Mrs Judy Gamin MLA, Member for Burleigh
DEPUTY CHAIRMAN:	Mr Darryl Briskey MLA, Member for Cleveland
MEMBERS:	Mr Frank Carroll MLA, Member for Mansfield
	Mr Ken McElligott MLA, Member for Thuringowa
	Hon Glen Milliner MLA, Member for Ferny Grove
	Miss Fiona Simpson MLA, Member for Maroochydore
RESEARCH DIRECTOR:	Ms Kerryn Newton
SENIOR RESEARCH OFFICER:	Mr David Thannhauser
EXECUTIVE ASSISTANT:	Ms Tania Jackman

CONTENTS

Page No.

CHAIRMAN'S FOREWORD

Information technology has been of great assistance to us in the preparation of this report. Much of the research has been conducted by the use of electronic databases. The itinerary for the committee's study tour to Canada, during which we met with people with respect to both bill of rights and privacy issues, was done through the Internet and via the convenience of instantaneous and paper-free e-mail. Needless to say, this report is not about trying to inhibit all of the economic and social conveniences of information and other technology from which we all benefit.

However, the genesis of this report came from our realisation that government has a responsibility to ensure that new developments in society do not flourish without a careful assessment of any consequences that may outweigh their benefits. Whilst the Queensland public and private sectors have been quick to find new ways in which technological developments can be employed, there has been no study in Queensland to date as to the potential intrusions on individual's privacy (whether information, personal, territorial or communications privacy) which may occur as a result.

In its 1990 *Report on Freedom of Information*, the former Electoral and Administrative Review Commission (EARC) recognised the increasing demand for legislation protecting personal privacy. Whilst EARC attempted in its report to promote the protection of information privacy, it stated that privacy principles were of such importance as to warrant comprehensive review and legislation. EARC therefore recommended that the Queensland government consider a review of privacy, either by it or a body established for that purpose, and the introduction of general privacy legislation.

We have effectively carried out that comprehensive review.

Just over a year ago, we resolved to conduct an inquiry into the adequacy of existing measures in Queensland which protect the privacy of individuals, and to consider whether the introduction of further measures to enhance the privacy of individuals is desirable. What followed was an extensive consultation and inquiry process in which we sought to hear from the people of Queensland as to where their privacy concerns, if any, emanated from.

The response clearly indicated that there are privacy concerns in the community which relate to all aspects of privacy - information, communications, territorial and personal privacy. However, clearly the first area to be addressed is the privacy of personal information afforded by Queensland government departments and agencies. Our approach therefore has been to establish a framework (or implement structural change) within which these priority concerns can be addressed.

The need for some form of information privacy regulation became more evident during the course of our inquiry. In November 1997, the Queensland Parliament referred to the committee the Criminal Law (Sex Offenders Reporting) Bill 1997 for consideration and report. The Bill proposed that persons who commit sex offences against children be required to report their personal details and details of their convictions in this regard to the police. The Bill further provided that the Police Commissioner may keep a sex offenders register which may include, amongst other matters, those personal details. Provision was also made for information from that register to be disclosed to certain persons.

We had a number of significant privacy concerns resulting from the provisions of that Bill. In particular, we noted that there were no principles governing the security, use, collection and disclosure of the information from that register. In recommendation 25 of that report, we recommended that:

> *…consideration be given to the serious privacy issues which arise with respect to the handling and integrity of personal information recorded on the sex offenders register. This is of particular concern given that Queensland currently does not have privacy legislation and/or a privacy guardian or advocate such as exists at the commonwealth level.*

As a result of our consideration we have recommended that a privacy regime be established in Queensland. This regime is to consist of the implementation of a consistent set of information privacy principles (IPPs) together with a new officer of the Parliament, the Queensland Privacy Commissioner (to be assisted by a privacy advisory committee). These principles, which are based on those contained in the *Privacy Act 1988* (Cth), regulate matters such as the collection, access, storage, use and disclosure of personal information. At least initially these principles are to apply to Queensland state departments and agencies, local governments, government contractors and GOCs. Both the Queensland Privacy Commissioner and the IPPs are to be established by a proposed Privacy Act (Qld).

Information privacy in the private sector, which is an area in which there has been much recent activity, is dealt with in a separate chapter. In the case of the private sector we recognise the compelling arguments for any regulation to be conducted on a national rather than a state-by-state basis.

In this report we also canvass other specific information privacy concerns (such as genetics and the use of smart cards) and *non-information* privacy concerns (such as surveillance), many of which are capable of being addressed at least to some extent within our proposed privacy framework.

Our final recommendation relates to the need to bring about cultural change with respect to privacy and the government's commitment to observing the rights and liberties of individuals as a fundamental legislative principle. This is set out in the *Legislative Standards Act 1992* (Qld). Whilst the right to privacy falls within these principles, we believe that regardless of whether our recommendations are ultimately adopted, the examples listed in that Act should be extended to include an example relating to privacy. This, we believe, will help to ensure that privacy issues are considered at the policy development and drafting stages of Queensland legislation.

The preparation of this detailed report has only been possible with the assistance of a number of people. We received a total of 81 submissions in relation to our inquiry, conducted two public hearings and one seminar. As a result we gathered a substantial amount of valuable material relevant to our inquiry and we thank all those who gave the committee written and oral submissions and who spoke at our seminar. Similarly, we refer in our report to the Canadian experience with respect to privacy. Much of this information is from meetings we had with privacy officials and experts in Canada and therefore we wish to thank those persons who kindly gave up their time to talk to us with respect to privacy regulation at the federal and provincial levels in Canada.

In some cases in this report we have recommended that the provisions in the proposed Privacy Act (Qld) be modelled on provisions that are currently contained in the Commonwealth *Privacy Act*. This is particularly so in relation to the IPPs themselves and the functions and powers of the Queensland Privacy Commissioner.

As we do not have first-hand experience regarding the day-to-day operation of the Commonwealth legislation, we engaged Mr Nigel Waters, Consultant in Fair Information Practices, to review and comment on relevant portions of our final draft report. Mr Waters was, until recently, effectively the deputy to the federal Privacy Commissioner since the *Privacy Act* 1988 came into force. Given his extensive experience in the federal Privacy Commissioner's office and in relation to privacy generally, we believe that Mr Waters' input has resulted in a report which is of the highest standard. We thank Mr Waters for his comments which he provided to us in the short time-frame required.

Of course, thanks must also go to the committee's research staff: our Research Director, Ms Kerryn Newton, our Senior Research Officer, Mr David Thannhauser and our Executive Assistant, Ms Tania Jackman. I also thank the members of the committee who have put in a substantial amount of time and effort in formulating what we believe to be a necessary privacy framework for Queensland.

This report consists of five parts.

- Part 1 - What is privacy, why it should be protected and how privacy is currently protected in Queensland and in comparative jurisdictions.
- Part 2 - Information privacy in the public sector.
- Part 3 - Information privacy in the private sector.
- Part 4 - Other specific information and non-information privacy concerns
- Part 5 - Conclusion.

We are confident that the recommendations contained in this report reflect a balanced, practical approach to the question of privacy protection in Queensland for today and tomorrow. We trust that our recommendations will meet with a timely response from government.

[Original Signed]

Judy Gamin MLA
Chair

2 April 1998

ABBREVIATIONS AND ACRONYMS USED IN THIS REPORT

AAT	Administrative Appeals Tribunal
ABA	Australian Bankers' Association
ADC-Q	Anti-Discrimination Commission, Queensland
AEC	Australian Electoral Commission
ALRC	Australian Law Reform Commission
AMA	Australian Medical Association
APC	Australian Press Council
ARC	Administrative Review Council
ASIO	Australian Security Intelligence Organisation
BSA	Building Services Authority
CCTV	closed circuit television
CJC	Criminal Justice Commission
CRU	continuous roll updating
DFYCC	Department of Families, Youth and Community Care
DPAC	Data Protection Advisory Council
EARC	Electoral and Administrative Review Commission
EBFG	Electronic Business Framework Group
ECQ	Electoral Commission, Queensland
EFT	electronic funds transfer
ESD	electronic service delivery
EU	European Union
EU Directive	1995 European Union *Directive on the protection of individuals with regard to the processing of personal data and on free movement of such data*
FACTS	Federation of Australian Commercial Television Stations
FLPs	fundamental legislative principles
FOI	freedom of information
GBEs	government business enterprises
GCCC	Gold Coast City Council
GOCs	government owned corporations
HREOC	Human Rights and Equal Opportunity Commission
ICAA	Institute of Chartered Accountants in Australia
ICCPR	International Covenant on Civil and Political Rights
IEC	institutional ethics committee

IPP	information privacy principle
LCARC	Legal, Constitutional and Administrative Review Committee
LCC	Logan City Council
LGOCs	local government owned corporations
LSA	Life, Investment and Superannuation Association
NOIE	National Office for the Information Economy
NHMRC	National Health and Medical Research Council
1998 'National Principles'	National principles for the fair handling of personal information
NSWLRC	New South Wales Law Reform Commission
OECD	Organisation for Economic Co-operation and Development
OECD Guidelines	OECD *Guidelines governing the protection of privacy and transborder flows of personal data*
PCEAR	Parliamentary Committee for Electoral and Administrative Review
PCJC	Parliamentary Criminal Justice Committee
PIN	personal identification number
PRPP	public register privacy principles
QAO	Queensland Audit Office
QCC	Queensland Crime Commission
QCCI	Queensland Chamber of Commerce and Industry
QCCL	Queensland Council for Civil Liberties
QLRC	Queensland Law Reform Commission
QPS	Queensland Police Service
QUT	Queensland University of Technology
RAQ	Retailers' Association of Queensland
SCAG	Standing Committee of Attorneys-General
SCAN	Smart Card Advisory Network
SCOCA	Standing Committee of Officials of Consumer Affairs
TCLS	Townsville Community Legal Service Inc
UDHGHR	Universal Declaration on the Human Genome and Human Rights
UDHR	Universal Declaration of Human Rights
UNESCO	United Nations Educational Scientific and Cultural Organisations

SUMMARY OF RECOMMENDATIONS

Recommendation 7 - The committee recommends that the Queensland Privacy Commissioner/Committee be able to modify the application of the IPPs by way of codes of practice to be promulgated as disallowable instruments. The committee further recommends that the provisions relating to codes of practice be modelled on those contained in Part VI of the *Privacy Act 1993* (NZ). 63

Recommendation 8 - The committee has already recommended that the Privacy Act (Qld) contain a set of IPPs substantially modelled on those contained in s 14 of the *Privacy Act 1988* (Cth). The committee confirms that it also recommends the inclusion of the exceptions contained in the Commonwealth IPPs in those IPPs, subject to the following comments.

Firstly, in relation to the 'public revenue protection' exceptions, the committee recommends that an additional balance mechanism should be introduced. This mechanism should be a certification process whereby a designated senior officer of the public revenue collection body seeking personal information from a department or agency must certify to the department or agency that that *particular* information is required for public revenue protection purposes.

Secondly, in relation to the law enforcement exceptions, the committee recommends that:

- the issues raised in the committee's consultation process and noted in the discussion above should be considered in the drafting of any law enforcement exceptions and, where appropriate, further consultation with law enforcement agencies should take place;

- there should be a certification process introduced whereby a designated senior officer of a law enforcement agency seeking personal information from a department or agency must certify to the department or agency that that *particular* information is required for law enforcement purposes; and

- any privacy regime should have regard to the protection of 'whistleblowers' and ensure that protection offered to them is not diminished.

In addition, the committee recommends that:

- the Privacy Act (Qld) contain a Part modelled on Part VI of the *Privacy Act 1988* (Cth) pursuant to which the Queensland Privacy Commissioner/Committee will have the ability to make public interest determinations; and

- the Queensland Privacy Commissioner/Committee conduct further inquiry and consultation with respect to the need and/or desirability of public register privacy principles such as those contained in Part VII of the *Privacy Act 1993* (NZ).....75

Recommendation 9 - On the basis that the IPPs in the Privacy Act (Qld) are substantially modelled on those contained in s 14 of the *Privacy Act 1988* (Cth), the committee recommends the following:

1. Those IPPs relating to:

- manner of collection of personal information (IPP 1);
- purpose for which personal information is collected (IPP 2); and
- accuracy and relevance of information collected (IPP 3);

apply to personal information collected *after* the commencement of the Privacy Act (Qld).

2. Those IPPs relating to:

- the storage and security of personal information (IPP 4);
- the maintenance of records kept by a record-keeper (IPP 5);
- access to records containing personal information (IPP 6);
- alteration of records containing personal information (IPP 7);
- the requirement for record-keepers to check the accuracy etc of personal information before use (IPP 8); and
- the requirement that personal information is only to be used for relevant purposes (IPP 9);

apply to personal information collected both *before and after* the commencement of the Privacy Act (Qld).

3. Provision be made for the IPPs regarding the use and disclosure of personal information (IPPs 10 and 11) to apply, as far as is reasonably practicable, to information collected both *before and after* the commencement of the Privacy Act (Qld).

4. Special provision be made in the case of the access principle (IPP 6) as it applies to certain health records, namely, that that principle will only apply to health services and records or entries made on an existing record where these occurred after the date of commencement of the Privacy Act (Qld). However, in cases where matters of fact are concerned, a person should have a right of access to these records whenever they were prepared.....80

Recommendation 10 - The committee recommends that, given the complexity of issues arising in considering the interrelationship between the *Freedom of Information Act 1992* (Qld) and the Privacy Act (Qld), the Information Commissioner be extensively consulted with in the drafting of the Privacy Act (Qld) and any consequential amendments to the *Freedom of Information Act 1992* (Qld).

- the Queensland Privacy Commissioner has a discretion to annually publish a Personal Information Digest as required by the equivalent of s 27(1)(g) of the *Privacy Act* (Cth); and

- for the purposes of the functions contained in the equivalent of s 27(1)(c) and (r) of the *Privacy Act* (Cth), the Queensland Privacy Commissioner is required to report to the Minister and to Parliament.

The committee further recommends that:

- a provision modelled on s 29 of the *Privacy Act 1988* (Cth) be contained in the Privacy Act (Qld); and

- the Queensland Privacy Commissioner should be primarily responsible for monitoring Queensland's law enforcement agencies with respect to privacy issues given the desirability for consistency and lack of duplication in this regard. However, this matter is to be further considered and reported upon by the Queensland Privacy Commissioner as a matter of priority upon that officer's appointment.....106

Recommendation 14 - The committee recommends that the Privacy Act (Qld) confer on the Queensland Privacy Commissioner the powers necessary to effectively and efficiently fulfil the Commissioner's functions under that proposed legislation including in particular:

- the power of access and entry to premises occupied by an agency either with consent of the occupier or by warrant;

- the power to initiate his/her own investigation in relation to an act or practice of an agency that may constitute an interference with the privacy of an individual;

- powers in relation to the investigation of complaints lodged by individuals including powers of determination and declaration (regarding matters such as compensation); and

- reporting powers.

Further, the committee recommends that these powers be broadly modelled on those powers available to the federal Privacy Commissioner under the *Privacy Act 1988* (Cth), subject to the following considerations.

Firstly, the committee recommends that appropriate amendments be made in relation to appeal and review mechanisms open to complainants. These amendments should reflect that decisions of the Queensland Privacy Commissioner are subject to both judicial review under the *Judicial Review Act 1991* (Qld) and merits review. The Committee recommends that, in determining which merits tribunal should hear matters brought under the Privacy Act (Qld), the Queensland government give further consideration to acting upon the recommendations of the former Electoral and Administrative Review Commission and the former Parliamentary Committee for Electoral and Administrative Review in this regard.

Recommendation 26 - The committee recognises that specific consideration needs to be given to issues associated with the privacy of health information, particularly in the private sector. However, it also recognises that any regulation in this regard should be nationally consistent.

Therefore, the committee recommends that the Queensland government supports the federal Privacy Commissioner's efforts, in line with the federal government's position, to reach agreement on a national scheme relating to information privacy in the private sector which includes both best practice privacy standards and effective supervisory, enforcement and complaint resolution mechanisms in all areas including health.

However, the committee also recommends that, once established, the Queensland Privacy Commissioner review the privacy protection afforded to health information in the private sector as a result of that scheme, and make any necessary recommendations for change. 171

Recommendation 27 - The committee believes that, while the IPPs themselves and the functions of the Queensland Privacy Commissioner that relate directly to the IPPs and information privacy should be restricted to information privacy matters, the Queensland Privacy Commissioner should explicitly be given jurisdiction to deal with non-information privacy concerns.

Accordingly, the committee recommends that the parameters of the following functions that were recommended for the Queensland Privacy Commissioner in chapter 7 of this report be extended to enable the Commissioner to address non-information privacy matters (that is, matters that involve no record of personal information):

- examining proposed legislation [mirroring the *Privacy Act* (Cth), s 27(1)(b)];
- researching and monitoring technological developments [s 27(1)(c)];
- publishing guidelines for the avoidance of privacy-intrusive acts or practices of an agency [s 27(1)(e)];
- providing advice to a Minister or an agency on matters relevant to the Act [s 27(1)(f)];
- conducting education [s 27(1)(m)];
- doing anything incidental to the preceding functions [s 27(1)(o)]; and
- reporting on matters that concern the need for, or the desirability of, legislative or administrative action [s 27(1)(r)].

This will ensure that the Queensland Privacy Commissioner has the capability to address both information and non-information privacy concerns that may arise in the future. 179

Recommendation 28 - The committee is concerned about the proliferation of the use of surveillance technology by both the public and private sectors.

Therefore, the committee recommends that the Queensland Privacy Commissioner, upon that Office's establishment, inquire into surveillance undertaken by the private and public sectors in Queensland. The Commissioner's inquiry should draw upon the consultation undertaken by, and the research and findings of, the New South Wales Law Reform Commission in relation to its current surveillance inquiry. 188

Recommendation 29 - The committee recognises that a number of privacy issues arise from the various existing and potential applications of smart cards and from the wider area of electronic commerce.

With respect to these issues in relation to departments and agencies covered by the Privacy Act (Qld), the committee:

- notes that smart card systems will be required to comply with the information privacy principles in the Privacy Act (Qld); and

- recommends that the Queensland Privacy Commissioner conduct an audit to establish the use or intended use of smart cards and:

    (a) provide relevant guidance as to any privacy issues arising as a result of that use; and

    (b) make recommendations as to any further regulation that might be required.

With respect to privacy issues arising as a result of smart cards and electronic commerce in the private sector, the committee reiterates that there must be national consistency in any privacy regulation and recommends that the Queensland government continue to support national moves that address these privacy issues in a timely and appropriate manner. 198

Recommendation 30 - The committee recommends that, given:

- the complexity of the issues associated with genetic testing and the collection and use of personal genetic information; and

- the national dimension of many of those issues;

the matter be the subject of further consultation and inquiry by the proposed Queensland Privacy Commissioner. However, this consultation and inquiry should be undertaken in light of developments at the federal level and in conjunction with relevant federal bodies. ... 208

PART 1

1. CHAPTER 1 - INTRODUCTION

1.1 THE COMMITTEE'S ESTABLISHMENT AND JURISDICTION

The Legal, Constitutional and Administrative Review Committee ('the committee' or 'LCARC') was established in 1995 pursuant to the *Parliamentary Committees Act 1995* (Qld). According to that Act, the committee has the following four areas of responsibility:

- administrative review reform (including considering legislation about access to information, review of administrative decisions, anti-discrimination and equal opportunity employment);
- constitutional reform;
- electoral reform; and
- legal reform (including recognition of Aboriginal tradition and Island custom under Queensland law and proposed national scheme legislation referred to the committee by the Legislative Assembly).[1]

In addition, the committee is to deal with issues referred to it by the Legislative Assembly or under another Act, whether or not the issue is within its area of responsibility.[2]

Clearly, the committee's areas of responsibility are wide-ranging and, with the exception of matters referred to the committee by the Legislative Assembly[3], it is a matter for the committee to determine which matters falling within its areas of responsibility it will determine to inquire into. In exercising this discretion the committee gives careful consideration to which matters it should accord priority.

1.2 THE DECISION TO EMBARK ON AN INQUIRY INTO PRIVACY

Since its inception the current committee has been aware of the increasing amount of concern expressed in the community regarding real and potential invasions of individuals' privacy.

The advent of the 'information age' means that technology allowing access to, and use of, information including personal information, is increasingly becoming part of our everyday lives. Technology now allows for the cheap and indefinite storage of data which can be retrieved at will and transmitted globally. As a result, media such as the Internet, e-mail, smart cards, multifaceted data programs and electronic banking provide many social and economic conveniences. However, the same technology also brings with it concerns for individuals with respect to matters such as the collection, use and security of their personal information.

---

1 ss 9-13.

2 s 8(2).

3 Matters can be referred to the committee under either s 8(2) or s 13(b) of the Act.

In addition, modern sophisticated audio and visual surveillance technology is increasing the manner in which individuals' communications and 'territorial' privacy may be infringed.

The number and variety of sectors, organisations and industries utilising this new technology is also expanding. Privacy concerns traditionally focussed on personal information held by the government: the fear of 'big brother'. However, today privacy is also very much an issue in relation to the private sector, particularly in areas such as the media, finance and those sectors utilising telemarketing and direct marketing.

Privacy surveys such as that carried out by the federal Privacy Commissioner in 1995[4] and *MasterCard International* in 1996[5] confirm that privacy is growing as an important issue to Australians. The federal Privacy Commissioner's 1995 survey showed that confidentiality of personal information held by government and business organisations ranked second to education as the most important social issue to persons. Privacy ranked higher than other social issues such as the economy and the environment. This reflected a change in attitudes from those expressed in a 1990 survey in which education, the economy and the environment all rated higher than privacy.[6]

Yet despite the importance of privacy to individuals and their concerns regarding the protection of their privacy Queensland, like many other jurisdictions, has a paucity of privacy regulation both in terms of legislative and non-legislative measures. Information or data technology, and in many cases surveillance technology, is clearly advancing more rapidly than means of regulating legitimate use of that technology. This is a matter which the committee saw, and still sees, as in need of immediate attention.

As a result, in December 1996 the committee resolved that in discharging its responsibility in respect of administrative review reform and legal reform, it would conduct an inquiry into the adequacy of existing measures in Queensland which protect the privacy of individuals, and consider whether the introduction of further measures to enhance the privacy of individuals is desirable.

1.3 THE COMMITTEE'S INQUIRY PROCESS

The committee deliberately did not at the outset define strict terms of reference for its inquiry into privacy. Given the wide range of areas in which privacy concerns arise, the committee wished to refrain from unduly limiting issues to be addressed prior to any public consultation.

Therefore, the committee decided that as the first phase of its inquiry, it would produce an issues paper outlining a wide range of privacy issues and call for public submissions upon its release.

In addition to the normal research undertaken in the preparation of such papers, in March 1997 the committee undertook a study tour to Canada as part of its inquiry into the former Electoral and Administrative Review Commission's *Report on Review of the Preservation and*

4 Federal Privacy Commissioner, *Community Attitudes to Privacy*, Information Paper Number 3, Human Rights and Equal Opportunity Commission, August 1995.

5 MasterCard International, *Privacy and payments: A study of the Attitudes of the Australian Public to Privacy - Summary and Findings*, 1996.

6 Federal Privacy Commissioner, 1995, op cit, p 7.

Enhancement of Individuals' Rights and Freedoms.[7] The committee also took this opportunity to meet with persons knowledgable of the privacy regimes currently operating in Canada.[8]

The committee released its issues paper on 'Privacy in Queensland' in May 1997. In that paper the committee identified 23 issues which persons making submissions to the committee could address. Further, in accordance with the committee's open approach noted above, the paper clearly encouraged persons to inform the committee as to any additional privacy concerns which they may have.

The inquiry was advertised extensively in state, regional and local newspapers as part of what the committee believes was one of the largest advertising campaigns ever conducted by a Queensland Parliamentary committee for an inquiry. At the same time, the committee conducted an extensive mail-out of its issues paper. Approximately 1300 papers were sent by direct mail to persons and organisations which the committee identified as having an interest in relation to the general issue of privacy. Access to the committee's issues paper was further enhanced by it being available on the Parliament's Internet site.

A high level of general interest in the issue of privacy was reflected by the substantial number requests for issues papers and the numerous requests made of the committee for media interviews. The committee also ultimately received a total of 81 submissions in relation to its inquiry. The committee has authorised the publication of, and tabled in Parliament, those submissions not specifically marked confidential.

A list of the persons and organisations who made submissions to the committee appears as Appendix A of this report.

Recognising that privacy was a matter affecting all Queenslanders and not just residents of Brisbane, the committee held public hearings in relation to its inquiry on the Gold Coast on 7 November 1997 and in Townsville on 14 November 1997.

The following persons gave evidence at those public hearings.

Gold Coast - 7 November 1997

NAME	**TITLE**	**ORGANISATION**
Dr Jean Collie (assisted by Dr Inglis Chern)	Medical Superintendent	Prince of Charles Hospital
Mr Patrick Quirk	Assistant Professor	Bond University
Ms Joanne Budgen	Solicitor	Tenants' Union
Mr Ross Clarke	Industrial Officer	Retailers' Association of Queensland

[7] Electoral and Administrative Review Commission, *Report on Review of the Preservation and Enhancement of Individuals' Rights and Freedoms*, Queensland Government Printer, Brisbane, 1993.

[8] Reference to privacy protection in Canada is made throughout this report. A summary of the persons with whom the committee met and the areas of discussion during its study tour to Canada is also contained in the committee's *Report on a study tour relating to the preservation and enhancement of individuals' rights and freedoms and to privacy*, Report No 6, Queensland Government Printer, 1997.

NAME	TITLE	ORGANISATION
Mrs Rita Carroll	Research Officer	Adoption Privacy Protection Group
Ms Doral Law	Research Officer	Adoption Privacy Protection Group
Mr Phillip Spencer	Director of Administration and Finance	Logan City Council
Mr Tony Davis	Manager - Management Services	Gold Coast City Council
Mr Paul Stevens	Director - Corporate Services	Gold Coast City Council

Townsville - 14 November 1997

NAME	TITLE	ORGANISATION
Mr Robert Daly	Principal Solicitor	Townsville Community Legal Service Incorporated
Mr Bill Mitchell	Welfare Rights Solicitor	Townsville Community Legal Service Incorporated
Mr Robert Elwell	Housing Resource Service Worker	Townsville Housing Resource Centre
Mr Tony Breadsell	Advocacy Support Worker	Independent Advocacy in the Tropics Inc.
Ms Ruth Venables	Principal Solicitor	North Queensland Women's Legal Service Inc.
Ms Lindy Edwards	Coordinator	Townsville Women's Shelter
Dr Tony Landgren	Director of Medical Services	Mater Private Hospital
Ms Jayne Finlay	Acting Senior Conciliator	Anti-Discrimination Commission
Ms Mary Vernon	Assistant Editor	Townsville Bulletin

The committee also arranged a public seminar with respect to privacy which was held on the evening of Monday 17 November 1997 at Parliament House, Brisbane.

Six distinguished speakers who represented a variety of organisations each with a different perspective on the issue of privacy spoke at the seminar. These speakers were as follows.

NAME	TITLE	ORGANISATION
Mr Ian Dearden	President	Queensland Council for Civil Liberties
Dr David Brereton	Director - Research and Coordination Division	Criminal Justice Commission
Dr Bob Brown	President	Australian Medical Association

NAME	TITLE	ORGANISATION
Professor Bill Caelli	Head - School of Data Communications Faculty of Information Technology	Queensland University of Technology
Mr Graham Jones	Queensland Manager	Insurance Council of Australia
Mr Nigel Waters	Vice President Privacy Consultant	Australian Privacy Charter Council

The committee has authorised the publication of, and tabled in Parliament, the Hansard transcripts of both hearings and the seminar.

The information contained in all oral and written submissions has greatly assisted the committee in its consideration of issues relating to privacy. The committee makes reference throughout this report to various comments made in, and conclusions drawn from, public submissions. In these and many other cases whilst not specifically recognised, public comment and opinion has helped to shape the committee's conclusions and recommendations.[9]

The committee takes this opportunity to thank all persons and organisations who gave their time to make written submissions to its inquiry and to those persons who kindly agreed to appear at its hearings and seminar.

1.4 THE PUBLIC RESPONSE TO THE INQUIRY AND THE COMMITTEE'S APPROACH

It became clear from early in the committee's inquiry that many persons and organisations do have concerns relating to privacy which they feel are not being adequately canvassed by Queensland's current law.

Consultation revealed that the majority of these concerns relate to the privacy of personal information, particularly that held, collected and used by Queensland government departments and agencies. However, concerns also clearly arise from, and in, other areas within both the public and private spheres.

The additional privacy concerns brought to the committee's attention included the following matters.

- Use, access and disclosure of information held by local governments.
- Use, access and disclosure of medical and health records in both the public and private sectors.
- The operation of 'tenancy databases' which are databases run by private companies and consist of a collection of information about 'problem' tenants for use by member real estate agents. The committee has been informed that often the information stored on these databases is incorrect and that tenants have no right of access to, or correction of, information held about them on these databases.

[9] Whilst the committee is unable to specifically refer to confidential submissions in this report, their content has been given the same consideration as all non-confidential submissions.

- Privacy issues associated with the provision of financial services particularly use, access and disclosure of personal information supplied to the financial sector.

- Security concerns surrounding credit cards, smart cards, electronic commerce and computer "hacking".

- The selling of personal information for commercial purposes, particularly direct marketing and telemarketing.

- Use, access and disclosure of information under current adoption laws.

- Use, access and disclosure of genetic-related information.

- Use, access and disclosure of information which adversely affects the safety of women particularly in the case of those women who have been subjected to domestic violence.

- Privacy issues relating to communications including the ability to identify callers' telephone numbers.

- Surveillance in public and private places (including the workplace, commercial premises, and public places such as malls).

- Privacy issues associated with activities of the media.

The committee's approach to addressing these concerns has been to canvass many of the threshold issues with respect to privacy and recommend the establishment of a framework for privacy regulation in Queensland. Many of the above concerns are capable of being addressed *within* this framework.

The committee also addresses in this comprehensive report other privacy concerns that do not, for a number of reasons, fall directly within this framework but which have been brought to its attention.

1.5 FORMAT OF THIS REPORT

The issue of privacy is complex and in preparing this report the committee has had to research, collate, analyse and consider a tremendous amount of literature and other material on the area. During the course of the committee's inquiry a number of important developments have also taken place in the area of privacy, particularly in relation to information privacy regulation in the private sector.

In the remainder of Part 1 of this report the committee summarises much of this material and outlines what it believes to be important background information to the remainder of the report and the committee's recommendations. These chapters relate to:

- what is meant by privacy and why privacy should be protected;

- how privacy is currently protected in Queensland and an assessment of whether this protection is adequate; and

- a study of privacy initiatives in other jurisdictions.

Following on from this discussion, the report deals with three main areas in what the committee sees as their proper order of priority.

- Part 2 - Information privacy in the public sector.
- Part 3 - Information privacy in the private sector.
- Part 4 - Other specific information and non-information privacy concerns.
- Part 5 - Conclusion.

2. CHAPTER 2 - PRIVACY AND PRIVACY PROTECTION

2.1 WHAT IS PRIVACY?

There is no single agreed-upon definition of privacy. This is evident from a study of the voluminous judicial and academic attempts to define this concept.[10]

In 1888 Judge Thomas Cooley described privacy as 'the right to be let alone'.[11] A more modern and narrower definition, which has since been accepted by the Canadian Supreme Court and the United States Supreme Court, was proposed by Professor Alan Westin in 1967. According to this definition:

> *Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.*[12]

The 'right' to privacy has been recognised, albeit not defined, at the international level. Article 12 of the *Universal Declaration of Human Rights* (UDHR) which was adopted by the General Assembly of the United Nations in December 1948 and Article 17 of the consequent *International Covenant on Civil and Political Rights* (ICCPR) of 1966 in almost identical terms state that no one shall be subjected to arbitrary and unlawful interference with his/her privacy, family, home or correspondence, nor to unlawful attacks on his/her honour and reputation. These articles further provide that everyone has the right to protection of the law against such interference or attacks.

The reason for the difficulty in finding universal agreement on a modern definition of privacy stems from the fact that 'privacy' is as broad as it is subjective in nature, depending on the views and values of the society in which one lives. In this context it is also a concept which is ever-changing in response to factors such as the rapid advancement of technology.

However, whilst a definition of privacy has not emerged, clearly categories of privacy have been identified. Although they have the tendency to overlap, these categories are generally recognised as follows.[13]

- Privacy of the person. It is widely accepted that an individual should have freedom in relation to their own body and that a high level of justification is required for a person to be subjected to body searches, or for their physical or behavioural characteristics to be otherwise monitored.
- Privacy of space or territory. This category recognises that people should have the right to conduct their personal affairs in certain private spaces, such as their homes, free from surveillance and that there should be some controls on people entering that private space or territory.

---

10 Some of these attempts are noted in B Gaze and M Jones, *Law, Liberty and Australian Democracy*, The Law Book Company Limited, Sydney, 1990, pp 328-329. See also G Tucker, *Information Privacy Law in Australia*, Longman Professional, Melbourne, 1992, pp 1-2.

11 Harvard Law Review, 1890, p 91 as cited in Tucker, ibid, p 1.

12 A F Westin, *Privacy and Freedom*, Atheneum, New York, 1967, p 7 as cited in Tucker, ibid, p 1.

- Privacy of communications. Communication, either oral or written, can be effected via an increasing variety of media, the most recent and significant of which is the Internet. Respecting privacy of communications means that (subject to the context and medium by which it occurs) people should be able to conduct their affairs without being subject to surveillance.

- Privacy of information. 'Information privacy' involves the notion that people, at least to some extent, should be able to regulate the use of information about themselves.

As is evident from section 1.4, the majority of submissions to the committee canvassed privacy concerns which fell within the 'information privacy' category.

2.2 WHY, AND TO WHAT EXTENT, SHOULD PRIVACY BE PROTECTED?

There are a number of arguments advanced as to why privacy in general should be protected. Some of these include the following.

Firstly, privacy may be viewed as essential to human dignity and a key value which underpins other key values such as freedom of association and freedom of speech.[14]

Secondly, privacy protection can be viewed as an integral part of a democracy which respects individual liberty.

> *A free and democratic society requires respect for the autonomy of individuals, and limits the power of both state and private organisations to intrude on that autonomy.*[15]

Thirdly, implementing measures that protect privacy will give effect to international obligations. For example, the ICCPR recognises the right to privacy and requires state parties to adopt measures necessary to give effect to the rights covered by the covenant.

Fourthly, in the case of information privacy in particular, economic reasons have prompted calls for increasing privacy protection. Governments and businesses which are both keen for their customers to use electronic services and engage in electronic commerce need to assure those customers that their information will not be misused. Such considerations extend to the international level with current moves to link trade to adequate privacy protection.[16] Thus, many argue that privacy concerns need to be addressed as part of the framework for Australia to partake in the global 'information economy'.[17]

---

13 See The (now 'Australian') Law Reform Commission (ALRC), *Privacy*, Report No 22, Australian Government Printing Service, Canberra, 1983, p 21, para 46. See also generally Gaze, op cit, pp 330-356 and E Longworth and T McBride, *The Privacy Act: A Guide*, GP Publications, New Zealand, 1994, p 3.

14 Refer to the preamble of the Australian Privacy Charter issued by the Australian Privacy Charter Council, December 1994.

15 Ibid.

16 In this regard reference should be made to discussion regarding the 1995 European Union *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data* referred to later in this chapter and in chapter 10 of this report.

17 See for example the comments of the federal Privacy Commissioner, *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector*, Consultation Paper, August 1997

However, privacy is not an absolute right. Determining the level of protection that privacy should be afforded is fundamentally a question of determining an appropriate balance between competing interests. On the one hand there are important reasons (including those outlined above) to protect the rights of individuals to their privacy whether it be of their person, communications or information concerning them.

On the other hand, these privacy rights have to be considered in the context of, and against, broader public needs. For example, it is in the public interest for the government to collect certain information about people in order to operate and plan more effectively. Private and commercial bodies, such as insurance companies, may also have a legitimate need to gather information about individuals in order to be able to effectively carry on their business.

It will be seen throughout this report that whilst careful consideration must be given to determining the appropriate balance between these competing rights, it is possible to achieve such a balance via a number of mechanisms in a privacy regime.[18]

2.3 A BRIEF HISTORY OF PRIVACY PROTECTION AND THE RECENT FOCUS ON THE PRIVACY OF INFORMATION

The committee does not intend to detail in this report the history of the law of privacy. This is canvassed extensively elsewhere.[19] However, a brief reference to this history does assist in understanding the development of current privacy protection in Australia and indicates where Queensland may look for guidance should it implement further privacy protection measures.

This study also reveals that the advent of the information age has brought about privacy concerns particularly in the area of 'information privacy'. Therefore, many recent privacy developments at both the international and national level have been in this area.

The origins of the law of privacy can be traced to 1890 when two leading American jurists published an article titled *The Right to Privacy*.[20] Following this article came the development of a tort of breach of privacy in the United States and, as already noted, from the end of World War II the creation of a number of international instruments, such as the UDHR and the ICCPR, which specifically recognise the right to privacy.

However, significant calls for privacy protection did not emerge until the 1960s with the advent of computers and the subsequent general concern about the collection of information by governments.

In Australia, the first attempts to regulate privacy occurred in the late 1960s and early 1970s and primarily related to regulating the use of listening devices. Then, in 1973, the *Morison Report*[21] on the law of privacy in Australia recommended a statutory privacy regime to include

---

at p iii. Professor Caelli also made this point at the committee's seminar on privacy, Transcript, Brisbane, 17 November 1997, p 11.

18 See in particular the discussion at section 6.4 of this report which deals with exceptions to compliance with an information privacy regime.

19 See Tucker, op cit, pp 12-20. The history on this section draws largely from Tucker's work.

20 This article by Warren and Brandeis appears at 4 *Harvard Law Review*, 1890, p 193 as cited in Tucker, op cit, p 12.

21 Morison, *Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys General*, No. 170, New South Wales Government Printer, 1973 as cited in Tucker, op cit, p 15.

an independent privacy committee and a co-ordinated network of privacy bodies throughout Australia. Although a comprehensive privacy regime did not result, the report did signify the start of a number of moves in the area of privacy. These included:

- attempts, albeit unsuccessful, in 1974 by both South Australia and Tasmania to pass privacy legislation which, via a statutory tort, sought to give individuals and companies a broad right of privacy; and

- the passing of the *Privacy Committee Act* in New South Wales in 1975[22] which established a privacy committee with jurisdiction in relation to broad categories of privacy.

In 1976 the federal government also asked the Australian Law Reform Commission (ALRC) to inquire into, and report on, 'the extent to which undue intrusions or interferences with privacy arise' in Australia and 'what legislative or other measures are required to provide proper protection and redress' against such intrusions.[23]

In 1983 the ALRC handed down its comprehensive report on privacy. However, it was not until 1988 and due to other intervening events that privacy legislation applying to information held by the Commonwealth public sector was introduced. The ALRC's recommendations and the provisions of the *Privacy Act 1988* (Cth) are dealt with in more detail in chapter 4 of this report.

In the 1970s and 1980s developments with respect to privacy also occurred in Europe.

A number of European jurisdictions enacted comprehensive legislation regarding data protection in the 1970s. These jurisdictions included Germany, France, Denmark and Austria.[24] Eventually, moves were made to create some uniformity in European data protection laws, the result being the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* which was issued by the Council of Europe on 28 January 1981.[25]

This move for uniformity was extended when, in 1981, the Organisation for Economic Cooperation and Development (OECD) published eight principles regarding information privacy. The OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (the OECD Guidelines) are primarily directed to regulating the collection, accuracy, use, disclosure, security and access to personal data. These guidelines have since been adopted in one form or another in the privacy legislation of the majority of western industrialised countries.[26] A copy of the OECD Guidelines appears as Appendix B.

In 1984 the *Data Protection Act* (UK) was also passed. This legislation followed the 1972 UK *Younger Committee*[27] report which looked at issues of privacy protection in the private sector

---

22 A similar 'Privacy Committee Act' was passed in Queensland in 1984. Both the New South Wales and Queensland Acts are discussed in further detail in chapters 3 and 4 of this report.

23 See the Terms of Reference of the ALRC's inquiry, op cit, pp xxxvi-xxxvii.

24 Tucker, op cit, p16.

25 Ibid.

26 The Australian government adopted the OECD Guidelines in 1984 and the principles in the *Privacy Act 1988* (Cth) are based on these guidelines.

27 United Kingdom, *Report of the Committee on Privacy*, HMSO, Cmnd.5012, 1972, as cited in Tucker, op cit, p 15.

and concluded that comprehensive legislation was not required. As a result, this Act regulates computer processing facilities in the public and private sectors by registration. The scheme is overseen by a Data Protection Registrar.

Thus, in the last fifteen years many jurisdictions, particularly in Europe, have passed information privacy laws covering both their public and private sectors. Other jurisdictions, including Australia and Canada, have introduced comprehensive legislation concerning the privacy of information held by their respective governments.[28] More recently there have been attempts by countries with privacy legislation covering their public sectors to extend the coverage of that legislation to the private sector. In particular, this has taken place in New Zealand, the Canadian province of Quebec, Taiwan and Hong Kong.

Mention of the international developments with respect to privacy would also not be complete without reference to the 1995 European Union *Directive on the protection of individuals with regard to the processing of personal data and on free movement of such data* (the EU Directive), which requires all fifteen member states to have in place consistent and comprehensive information privacy laws by October 1998.

The Directive will also make it mandatory from October 1998 for European Union member countries to restrict the transfer of personal data to any country that does not have 'adequate' information privacy laws.

Given the potential impact of the EU Directive with respect to privacy protection particularly in the private sector, it is discussed in more detail in chapter 10 of this report.

[28] This Australian and Canadian legislation is discussed in more detail in this chapter 4 of this report.

3. CHAPTER 3 - QUEENSLAND'S CURRENT PRIVACY LAWS AND THEIR ADEQUACY

3.1 INTRODUCTION

In order to make an assessment as to the need for further privacy protection in Queensland, it is first necessary establish what privacy protection is currently afforded in Queensland and to assess in what areas that protection is, if at all, inadequate.

3.2 PRIVACY PROTECTION AT COMMON LAW

The common law in Australia (including Queensland) protects various 'rights' and interests of individuals although it has not as yet developed a 'right' to privacy. As noted by Latham CJ in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor and Others*:

> *The claim under the head of nuisance has also been supported by an argument that the law recognizes a right of privacy which has been infringed by the defendant. However desirable some limitation upon invasions of privacy might be, no authority was cited which shows that any general right of privacy exists.* [29]

This can be contrasted with the common law in the United States where a tort of breach of privacy has developed. A tort of privacy allows a person to bring an action in the courts against another person for a breach of their privacy.

However, some limited privacy protection is afforded at common law (and in equity) in Australia by laws such as those relating to defamation, breach of confidence and trespass.[30] Certain relationships also give rise to a duty of confidentiality such as that of doctor and patient, lawyer and client and banker and customer. In addition, contracts may include terms which relate to the protection of confidential information.

3.3 QUEENSLAND PRIVACY LEGISLATION TO DATE

3.3.1 The Invasion of Privacy Act 1971 (Qld)

Queensland in fact introduced the first specific piece of legislation dealing with privacy in Australia; the *Invasion of Privacy Act 1971* (Qld). However, the privacy protection offered by this legislation is limited.

The only 'information privacy' protection provided by the Act is in relation to access to, and disclosure of, reports of credit reporting agents.[31]

The Act also protects some 'communications privacy' by making it an offence to use a listening device to record or listen to a private conversation, or to communicate or publish any private

---

29 See *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor and Others* (1937) 58 CLR 479, pp 495-496.

30 For a detailed exposition on privacy protection at common law see Tucker, op cit, pp 21-58.

31 See generally Part 3, Division 2 of the Act.

conversation that has been overheard or listened to unlawfully.[32] Further, 'territorial privacy' is protected by the legislation in that it is an offence for any person to enter a dwelling house without the consent of the lawful occupier or owner, or to enter a dwelling house by force, threat, deceit or false representations whether or not with the consent of the lawful occupier or owner.[33]

3.3.2 The Privacy Committee Act 1984 (Qld)

More comprehensive privacy legislation was passed in 1984 by the Queensland Parliament. The *Privacy Committee Act 1984* (Qld) represented a modified version of the New South Wales legislation of the same name. This Act established a privacy committee consisting of seven members appointed on the recommendation of the Minister by the Governor-in-Council.[34]

The functions of the committee were set out in s 17 of the Act. That section provided that subject to the Act, the committee:

> *(a) may conduct research and collect and collate information in respect of any matter relating to the privacy of persons referred to it by the Minister;*
>
> *(b) may and, if directed by the Minister so to do, shall make reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interests of the privacy of persons;*
>
> *(c) may and, if directed by the Minister so to do, shall in relation to any matter relating to the privacy of persons generally disseminate information and undertake educational work;*
>
> *(d) may receive and investigate complaints about alleged violations of the privacy of persons.*

If the committee did receive and investigate a complaint about an alleged violation of privacy then the committee could only report in relation to that matter to the Minister.[35] Moreover, if upon conclusion of an investigation into such a complaint the committee believed that some further action was warranted, it could only advise the complainant that a report had been furnished to the Minister. It could not advise the complainant of the contents of the report.[36] Any report, or part thereof, prepared by the committee in accordance with its other functions could only be published with the approval of the Minister.[37] Thus, the committee enjoyed little independence from the Executive arm of government.[38]

For the purpose of conducting an investigation regarding a complaint about an alleged violation of the privacy of a person, the committee was given certain powers. These included the power to require any person to give or produce to a member of the committee: any

---

32 See ss 43-44.

33 s 48A.

34 Section 5(3) required the Minister to only recommend persons who, in his opinion, had a special knowledge of, or interest in, matters affecting the privacy of persons.

35 s 17(2).

36 s 17(3).

37 s 17(4).

38 Indeed, Tucker suggests that the introduction of the Queensland *Privacy Committee Act* was 'little more than the payment of lip service to the Orwellian spectre': G Tucker, 1992, op cit, p 71.

statement of information; any document or thing; or a copy of any document.[39] In the case of a person appearing before the committee, the committee could also require that person to answer any question.[40]

In accordance with a statutory requirement, the committee reported to Parliament each year in the form of an annual report.[41] These reports reveal that the committee's activities extended to all categories of privacy. The committee was also required to report prior to the expiration of a sunset period which fell due in 1991.[42]

In its last annual report and its final report, the committee mapped out its view on where the future of privacy protection in Queensland needed to head. In particular, the committee noted that information privacy was the area in which there was greatest public concern and that the Commonwealth Parliament had passed information privacy legislation binding its agencies.

> *This Committee considers it is appropriate such principles be legislatively set out and made applicable at least to Government agencies and there seems to be no great reason why they should not have application generally to those bodies which have information of a sensitive nature - for instance credit reference bodies, finance companies etc.*
>
> *It is noted that the Electoral and Administrative Review Commission has recommended legislation on privacy and this Committee considers that there is a need for a review of the present Invasion of Privacy Act which is very limited in its scope. We consider that the basic areas of privacy which are namely -*
>
> *(a) Territorial privacy;*
>
> *(b) Personal privacy;*
>
> *(c) Information privacy; and*
>
> *(d) Communication and Surveillance privacy*
>
> *should be given legal recognition and appropriate remedies available for any substantial and unlawful interference of those rights.*[43]

In these reports, the committee also addressed what the terms of reference for the then proposed new Queensland Privacy Committee should provide.[44] Broadly, these recommendations sought to give the committee wider functions and powers and more autonomy from the Minister. They further sought to ensure that the committee's membership would represent a cross-section of appropriate members of the community. The committee also recommended that in order for the proposed committee to carry out its functions effectively it needed adequate staffing and budgetary allocation.

---

39 s 19(1).

40 s 19(1).

41 s 20.

42 The initial sunset clause in the Act provided that the Act would expire 5 years from the date of proclamation and the Act was proclaimed on 22 August 1985 (s 29). However, this period was extended to 14 June 1991 by s 3 of the *Privacy Committee Act Amendment Act 1990* (Qld).

43 Queensland Privacy Committee, *The Sixth Annual Report of the Privacy Committee*, March 1991, p 3.

44 Ibid, p 8 and Queensland Privacy Committee, *The Final Report of the Inaugural Privacy Committee*, May 1991, particularly Appendix A.

In terms of the focus of a future Queensland Privacy Committee, the outgoing committee expressed the view that the most immediate need for activity appeared to be in the area of information privacy in the government sector. The committee also believed that the role of a new committee should extend to the private sector, particularly in those areas where large databanks of information on individuals are held.[45]

A subsequent Queensland Privacy Committee was never established. The recommendations of the committee concerning privacy legislation were also not acted upon.

3.3.3 Other relevant legislation in Queensland

In discussing current measures to protect privacy in Queensland it is relevant to refer to two other pieces of legislation which concern administrative law.

Firstly, with respect to access (or restrictions on access) to information it is appropriate to mention the *Freedom of Information Act 1992* (Qld) (the FOI Act.) In line with its objective of enhancing the accountability and transparency of government, the FOI Act confers a legally enforceable right to the community to obtain access to documents of an agency or an official and documents of a minister, subject to certain exemptions and exceptions. The Act enables members of the community to ensure that documents held by government concerning their 'personal affairs' are accurate, complete, up-to-date and not misleading.[46] Two observations relevant to privacy can be made with respect to the FOI Act.

As already noted, rights of access to and amendment of, personal information are generally recognised as 'information privacy rights'. The FOI Act protects the privacy of certain information to the extent that s 44 of the Act exempts from disclosure to third persons 'information concerning the personal affairs of a person' unless its disclosure would, on balance, be in the public interest.

Further, Part 4 of the Act sets out the procedure whereby persons who have had access to a document from an agency or Minister containing information relating to a person's personal affairs (or the personal affairs of a deceased person to whom the person is next of kin), may apply to the agency or the Minister for correction or amendment of any part of the information it if is inaccurate, incomplete, out-of-date or misleading.[47] (The interrelationship between FOI and privacy legislation is canvassed further in section 6.6.2 of this report).

Secondly, the *Parliamentary Commissioner Act 1974* (Qld) establishes the Office of the Parliamentary Commissioner for Administrative Investigations (the Ombudsman). The principal function of the Ombudsman is to investigate any administrative action taken by, in, or on behalf of, an agency.[48] 'Administrative action' is defined in s 4(1) of the Act to mean any action relating to a matter of administration including 'a decision and an act'. 'Agency' is defined in the same section to include a department, a local government or a public authority.

Therefore, it is possible that individuals who allege an agency has breached their privacy by an act or decision can lodge a complaint with the Ombudsman. The difficulty remains, however,

45 See particularly *The Final Report of the Inaugural Privacy Committee*, Appendix A, p 3.
46 Refer to the long title and ss 4-5 of the Act.
47 s 53.
48 s 13(1).

that there are no guidelines or standard against which to claim a 'breach'.[49] Further, the Ombudsman's powers are restricted to making recommendations in reports. The Ombudsman is also precluded from investigating the administrative action of certain bodies and persons.[50]

3.3.4 Recent recognition of the need to protect privacy in Queensland

Whilst there has not been specific legislative action in Queensland with respect to privacy since the former *Privacy Committee Act*, there has been recognition of the need for such a move. This is in addition to the comments made by the final Queensland Privacy Committee.

As noted by Fitzgerald QC in his landmark 1989 report:

> *In spite of our international obligations and the importance of the issue, the development of comprehensive legislation to protect individuals from breaches of personal privacy by either government or non-government organizations has been slow.*[51]

The issue of privacy was also raised in a number of the Electoral and Administrative Review Commission's (EARC's) reports.

In its 1990 *Report on Freedom of Information*[52] EARC stated that it was aware of the increasing demand for legislation protecting personal privacy and that whilst it had attempted in its report to promote the protection of information privacy, privacy principles were of such importance as to warrant separate review and legislation. Thus, EARC recommended that the government should consider a review of privacy and the introduction of general privacy legislation.[53]

Later in its 1993 *Report on Review of the Preservation and Enhancement of Individuals' Rights and Freedoms*[54], EARC recommended that Queensland adopt a bill of rights and that it include a general right to privacy similar to that in the ICCPR. However, whilst that right seemingly covered territorial, personal and communications privacy it did not deal specifically with information privacy.[55] EARC's recommendations in this regard have not been implemented although the committee is also currently conducting an inquiry which encompasses a review of EARC's 1993 report.[56]

A number of recent policy statements have also been made regarding privacy.

In June 1995 the former Goss Government directed an interdepartmental working group be established to give consideration to certain privacy matters. That group forwarded its report to

---

49 Refer also to section 6.2.1 of this report for further discussion on the Ombudsman.

50 s 13(5).

51 G E Fitzgerald, *Report of a Commission of Inquiry Pursuant to Orders in Council*, Queensland Government Printer, 1989, p 174.

52 EARC, *Report on Freedom of Information*, Queensland Government Printer, December 1990.

53 Ibid, paras 9.35-9.39.

54 EARC, *Report on Review of the Preservation and Enhancement of Individuals' Rights and Freedoms*, Queensland Government Printer, August 1993.

55 Ibid, para 8.339.

56 Queensland Parliament. Legal, Constitutional and Administrative Review Committee, *The Preservation and Enhancement of Individuals' Rights and Freedoms: Should Queensland Adopt a Bill of Rights?*, Issues Paper No 3, Queensland Government Printer, September 1997.

the then Attorney-General in December 1995, although apparently it was not considered prior to the change in state government in early 1996.

The current Queensland Coalition government in its 1995 election campaign also outlined a privacy policy which included the establishment of an independent statutory privacy commissioner who would, amongst other functions, establish and enforce guidelines for the collection, use and storage of personal information (based on the OECD Guidelines) for state government agencies and departments.[57]

Legislation in accordance with this statement has not yet been forthcoming.

3.4 THE ADEQUACY OF QUEENSLAND'S PRIVACY LAWS

3.4.1 General assessment

The preceding discussion regarding current privacy protection in Queensland reveals that this protection is limited to:

- indirect protection by the common law;
- very limited protection of territorial, information and communications privacy by the *Invasion of Privacy Act 1971* (Qld); and
- the access and amendment provisions and the 'personal affairs' exemption in the FOI Act.

Some privacy protection is also afforded by confidentiality provisions contained in miscellaneous legislation[58] and legislative controls on police powers with respect to surveillance.[59]

The discussion also reveals that in Queensland:

- there is no privacy legislation governing information privacy in state government departments or agencies;
- there is no privacy legislation governing information privacy in the private sector;
- there is limited privacy legislation governing other non-information privacy concerns in the public and private sectors; and
- there is no privacy guardian or advocate to monitor the protection of individuals' privacy in general.

---

57 See the document titled *National and Liberal Parties Policy on Privacy*.

58 For example, s 10(1) of the *Criminal Offence Victims Act 1995* states that a victim's privacy shall be protected. The Criminal Justice Commission and Queensland Police Service also have confidentiality obligations under their relevant legislation.

59 See, for example, the *Police Powers and Responsibilities Act 1997* and the *Drugs Misuse Act 1986*. Surveillance is discussed further in section 11.3 of this report.

The question therefore arises as to whether this current situation is failing to address privacy concerns.

3.4.2 Arguments raised in public consultation

Submissions in response to matters raised in the committee's issues paper revealed that many persons and organisations do have concerns relating to privacy protection which they feel are not being adequately canvassed by Queensland's current law, and therefore need to be addressed by further legislative and/or administrative action.

The general areas of these concerns have been listed in section 1.4 of this report. What is evident from this list is that the majority of these concerns relate to the privacy of personal information. In other words, many people do not believe that there are adequate measures regulating the collection, storage, use, access, and disclosure of their personal information (such as their name, address, date of birth etc.) by persons and organisations who hold that information.

Consultation also revealed that these concerns arise particularly in the context of information held by state government departments and agencies. In fact, some departments themselves recognised the need for this area to be addressed.

In a joint submission Main Roads and Queensland Transport noted:

> *Both departments have concerns relating to privacy protection that hopefully will be addressed if the government implements some form of privacy regime. Queensland Transport is responsible for the custody and maintenance of 2.2 million drivers licence records and 4.5 million vehicle registration records. Both Main Roads and Transport have systems that record various personal details of members of the public and departmental staff, including - name and address, dates of birth, bank account details, salary information, property values and criminal history searches on individuals.*
>
> ***While the departments have policies in place to try and protect the privacy of this information and ensure its appropriate use, the absence of state legislation adds difficulties to the development and enforcement of these policies.*** [Emphasis added.][60]

The Department of Families, Youth and Community Care (DFYCC) also made the following comment:

> *In the context of community expectations the current law in Queensland is not adequate with respect to privacy protection.*
>
> ***Ironically many of the most sensitive personal records are held by state government agencies. However unlike records held by the Commonwealth there is no legislation which specifically addresses the need for information privacy protection****. With the operation of Freedom of Information legislation in both jurisdictions it has become apparent that there is an expectation in the community that information privacy regimes should operate in both jurisdictions*. [Emphasis added.][61]

---

60 Joint submission by Main Roads and Queensland Transport dated 28 July 1997, p 1.

61 Department of Families, Youth and Community Care, submission dated 12 August 1997, pp 1-2.

Dr Brereton speaking on behalf of the CJC at the committee's privacy seminar also noted that Queensland's current privacy laws are inadequate and that most government departments and agencies had themselves attempted to offer some privacy protection in the absence of legislation.

> *…most Government agencies have internal rules on the handling of confidential personal information, and a number, such as the CJC and the Queensland Police Service, have statutory obligations requiring them to ensure confidentiality.* ***But really there is a lack of uniformity in approach across the agencies, and there are many gaps and areas of uncertainty in the regulatory framework***. [Emphasis added.][62]

Those submissions which did conclude that Queensland's privacy laws were adequate and that therefore further administrative and legislative action with respect to privacy is not necessary, primarily related to the private sector and, in particular, the banking sector.

The Queensland Chamber of Commerce and Industry believed that in the absence of 'incontrovertible evidence to the contrary' the current law is adequate.

The Australian Bankers' Association also submitted:

> *In so far as the banking sector is concerned, it is submitted that the combination of common law, contract law and Part IIIA of the Privacy Act together provide a strong basis for the protection of privacy of the individual in Queensland (and throughout Australia).*[63]

The adequacy of privacy laws in the context of the private sector is dealt with in more detail in chapter 10 of this report.

3.4.3 Analysis and conclusion

Consultation clearly revealed that many do not believe that the current law with respect to privacy in Queensland adequately addresses privacy concerns. The most pressing of these concerns seem to relate to the collection, use, access and disclosure of personal information held by state government departments and agencies.

State government departments and agencies hold vast amounts of personal information, much of which is very sensitive. This includes information such as that relating to individuals' health, family history, addresses and other contact details, drivers' histories and criminal histories.

Currently there is no legislative or overall administrative regulation (other than ad hoc self-regulation) preventing the misuse of this information. The fact that some departments themselves recognise that legislation is needed in order to develop and enforce privacy guidelines reinforces the need for this area to be addressed in the very short term.

In this regard the response received by the committee reflected similar observations made elsewhere including:

---

62 Transcript, 17 November 1997, p 5.

63 Australian Bankers' Association, submission dated 30 July 1997, p 8.

- the results of the federal Privacy Commissioner's 1995 survey[64] and *MasterCard International's* 1996 survey[65] which found that government agencies which have computer access to networks of personal information were seen to pose the biggest threat to privacy;

- the comments made by the former Queensland Privacy Committee that the most immediate need for activity by any future Queensland privacy committee appears to be in the area of information privacy in the government sector[66]; and

- the 1994/95 annual report of the New South Wales Privacy Committee which shows that the third greatest percentage of written complaints in 1994/95 related to complaints about government departments.[67]

The committee agrees that the issue of information privacy in Queensland's public sector is an area which should be considered as a matter of priority. Further, it believes that a number of other factors support additional protection of information privacy in this regard.

Firstly, in many cases the law obliges individuals to provide to state government departments or agencies much personal information. The fact that individuals do not have the ability to 'opt out' of providing personal information, in the committee's opinion, places a higher onus on the recipient of that information to ensure that it is not misused.

Secondly, technology which enhances data processing capabilities, and hence service delivery, is increasingly being used by government departments and agencies. Therefore, there must be systems in place which assure individuals that their privacy is being protected by equivalent technology.

As the Victorian government has recognised with projects such as its Electronic Service Delivery project (which aims to provide a 'single integrated electronic face of government'), the law has an important role to play in this new technology infrastructure. In a recent speech Mr Victor Perton MP noted:

> *[The law] will be the primary means by which the community can be reassured that its interests, for example in the area of privacy, are balanced against competing government or commercial interests. Privacy regimes must therefore form part of the infrastructure of our new information-based society.*[68]

Thirdly, it is clear that an information privacy scheme for the state public sector is consistent with 'best practice' standards in public administration. An information privacy regime should not only increase the quality of information stored but should also improve the quality of action taken on the basis of that information.

Finally, the Queensland government has made a legislative commitment to recognising individuals' rights and freedoms. Section 4 of the *Legislative Standards Act 1992* (Qld)

---

64 Federal Privacy Commissioner, 1995, op cit, p 11.

65 MasterCard International, 1996, op cit, p 12.

66 Refer to the discussion above in section 3.3.2.

67 Privacy Committee of New South Wales, *Annual Report 1994/95*, Sydney, p 34. In 1993/94 the greatest percentage of written complaints related to government departments. The establishment and functions of this committee are described in more detail in chapter 4 of this report.

68 V Perton, 'A Privacy Act for Victoria?' Paper presented to the Australian Institute of Administrative Law seminar, *Private Sector Privacy*, Melbourne, 26 February 1997, p 14.

requires legislation to have sufficient regard to the 'fundamental legislative principles' (FLPs), which are stated to be 'the principles relating to legislation that underlie a parliamentary democracy based on the rule of law'. These principles, amongst other matters, require that legislation has sufficient regard to the 'rights and liberties of individuals'.

Additional measures recognising and defining the right to privacy in Queensland will assist our policy and law makers in complying with the FLPs. These measures should also, in turn, bring about a significant cultural and attitudinal change within at least the public sector to be more privacy orientated.

The *Privacy Act 1988* (Cth) which primarily concerns the protection of privacy of personal information held by Commonwealth agencies, remains as the most significant piece of privacy legislation in Australia, yet for constitutional reasons it does not and can not provide any protection for the privacy of personal information held by state governments. It is a matter therefore for the Queensland government as to what legislative or administrative action it will take in this regard.

The conclusion that the most pressing concern with respect to privacy is the privacy of personal information held by state government departments and agencies does not mean that the committee does not have concerns about other areas in which privacy issues arise. Later in this report the committee deals with information privacy in the private sector and some other specific information and non-information privacy concerns.

However, the committee believes that the logical approach is to first bring about structural change by introducing systems within which the most pressing privacy concerns can be addressed. Additional privacy protection measures may well then be built upon and into these basic structures.

3.4.4 Recommendation

Recommendation 1 - The committee concludes that Queensland's current law with respect to protecting individuals' privacy is inadequate and that there are valid privacy concerns which need to be addressed by legislative and/or administrative action.

Therefore, the committee recommends that the Queensland government introduces measures to ensure the greater protection of individuals' privacy. In particular, the committee recommends that the privacy protection of personal information held by Queensland government departments and agencies is addressed as a matter of priority.

(The committee's recommendations as to what these measures should be are discussed in the following chapters of this report.)

4. CHAPTER 4 - PRIVACY INITIATIVES IN OTHER JURISDICTIONS

4.1 INTRODUCTION

In the previous chapter the committee concluded that measures needed to be introduced in Queensland to ensure the greater protection of individuals' privacy, particularly in relation to personal information held by state government departments and agencies.

The committee has studied privacy initiatives in various other jurisdictions in order to seek some guidance as to what these measures might be and, more particularly, to establish the influence, if any, that Commonwealth efforts in this area may have on privacy protection in Queensland.

In this chapter the committee summarises this research. Much of the material in this chapter provides important background material to the discussion and recommendations made later in this report.

4.2 COMMONWEALTH PRIVACY LEGISLATION AND DEVELOPMENTS

On an international level Australia has undertaken two significant steps acknowledging the importance of the right to privacy.

Firstly, in 1980 Australia ratified the ICCPR which, as previously discussed, includes a right to privacy. Whilst the act of ratification does not mean that the covenant has become part of Australia's domestic law, ratification does mean that Australia has committed itself to adopt such legislative or other measures necessary to give effect to the rights contained in the covenant.[69]

In 1991 Australia also ratified the First Optional Protocol to the ICCPR. The protocol enables individuals who claim that their rights as set out in the Covenant have been violated and who have exhausted all domestic remedies, to complain to the United Nations Human Rights Committee. The avenue of appeal is thus open to all Australians. In fact, the first complaint lodged by an Australian pursuant to this protocol concerned a breach of privacy and was upheld by the Human Rights Committee.[70]

Secondly, Australia is a member of the OECD which, it will be recalled, recommended that member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines annexed to its recommendation. (These have previously been referred to as the OECD Guidelines.)[71]

---

69 See article 2(1) & (2) of the ICCPR.

70 See *Toonen v Australia*, Communication No 488/1992 (UN Doc CCPR/C/50/488/1992). Toonen alleged that the Tasmanian criminal law on homosexual conduct violated his right to privacy under Art 17(1) of the ICCPR and his right to be protected against discrimination under Art 26. The committee upheld his claim.

71 See the preamble to the *Privacy Act 1988* (Cth).

Australia has, at least to the extent of information privacy in the public sector, taken legislative action in fulfilment of its international obligations under the ICCPR and OECD Guidelines via the enactment of the *Privacy Act 1988* (Cth).

4.2.1 The Privacy Act 1988 (Cth)

Following a long inquiry process, the Australian Law Reform Commission (ALRC) released a detailed report on privacy in Australia in 1983. In this report the ALRC recommended that the Commonwealth Parliament enact comprehensive privacy legislation which, amongst other matters, sought to establish a Privacy Commissioner and provide persons with a right of access to, and amendment of, personal information held in the Commonwealth public sector.[72]

However, it was not until 1988 that Commonwealth privacy legislation was passed. The *Privacy Act 1988* (Cth) in part emanated from the 1983 ALRC report and in part from an attempt to pass the Privacy Bill of 1986. This later Bill enhanced the powers given to the Privacy Commissioner proposed in the ALRC's draft privacy legislation and charged the Commissioner with the responsibility of investigating alleged breaches of eleven information privacy principles (IPPs) by Commonwealth government agencies. The fact that this Privacy Bill was tied to then unsuccessful Australia Card Bill 1986 meant that it was not passed. However, a further attempt to pass a Privacy Bill in 1988 to provide a measure of privacy protection to accompany the introduction of tax file numbers eventually succeeded.[73]

In addition to regulating the use of tax file number information, the *Privacy Act* imposes on Commonwealth and ACT agencies a duty not to do an act or engage in a practice that breaches one or more of eleven information privacy principles (IPPs).[74] A copy of the IPPs as they appear in s 14 of the *Privacy Act* are attached as Appendix C.

The IPPs contained in the *Privacy Act* (Cth) are based on the OECD Guidelines and thus they regulate the collection, storage, security, use, access, disclosure and correction to 'personal information' held by an 'agency'. 'Personal information' is defined in the Act to be information or an opinion, whether true or not, about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.[75] 'Agency' is defined to include a Minister, department and certain bodies or tribunals established or appointed for a public purpose.[76]

Whilst the Act primarily relates information privacy in the Commonwealth public sector it does also apply to the private sector to a limited extent. As well as regulating the use of tax file numbers throughout the community from commencement, the *Privacy Amendment Act 1990* (Cth) extended the operation of the Act to credit reporting agencies and credit providers with respect to personal credit information.[77]

---

72 Australian Law Reform Commission, 1983, op cit. The ALRC's Draft Privacy Bill 1983 also sought to regulate body cavity searches and secret surveillance.

73 Tucker, op cit, pp 73-74. The *Privacy Act 1988* (Cth) commenced operation on 1 January 1989.

74 s 16.

75 s 6.

76 s 6.

77 See Part IIIA of the Act.

In addition, the Privacy Amendment Bill 1998 (Cth) which was introduced into the House of Representatives on 5 March 1998 seeks to amend the *Privacy Act* (Cth) to apply it to personal information held by contractors in relation to services provided by the Commonwealth government.[78]

The *Privacy Act* (Cth) also establishes the office of the federal Privacy Commissioner who is prescribed a number of functions aimed at ensuring compliance with the legislation. These functions include investigating complaints, monitoring technological trends for adverse effects on individuals' privacy, and educating members of the public as to individuals' privacy rights.[79]

Further detail on specific provisions in the *Privacy Act* (Cth), including those provisions concerning the federal Privacy Commissioner's functions and powers, are detailed later in this report.

4.2.2 A national uniform privacy scheme

In its 1983 report, the ALRC noted the importance of a national approach to the protection of privacy, at the very least in relation to information practices, and indicated that its proposals for privacy legislation could form the basis of a national privacy scheme.[80] Whilst this has not eventuated and the *Privacy Act* remains as the most significant privacy legislation in Australia today, there have been recent calls for a national approach to privacy.

In the main these calls have arisen because now vast amounts of personal information are also held by private sector agencies. In addition, as the demarcation between the public and private sectors is gradually blurring, it is increasingly difficult to apply and justify different privacy standards for each sector.

The House of Representatives Standing Committee on Legal and Constitutional Affairs, in its report titled *In Confidence: A report of the inquiry into the protection of confidential personal and commercial information held by the Commonwealth*[81], recommended the extension of the IPPs to the private sector.[82] The Australian Law Reform Commission and Administrative Review Council in a joint report on the Commonwealth *Freedom of Information Act 1982*[83] also recommended that an information privacy regime should be applicable to both the public and private sectors.

In September 1996, the federal Attorney-General released a discussion paper titled *Privacy Protection in the Private Sector* which outlined a possible co-regulatory approach to privacy protection in the private sector. The proposal, if implemented, would have seen national privacy legislation covering the private sector.

---

78 The extension of privacy legislation to service providers contracted by the government is dealt with in more detail in chapter 8 of this report.

79 These functions are set out in ss 27, 28 and 28A of the Act and are discussed more fully in chapter 7 of this report.

80 ALRC, 1983, op cit, vol 2, p 28, para 1092.

81 House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A report of the inquiry into the protection of confidential personal and commercial information held by the Commonwealth,* Australian Government Printing Service, June 1995.

82 Ibid, pp 172-173.

83 Australian Law Reform Commission (Report No. 77) and Administrative Review Council (Report No. 40*), Open government: A review of the federal Freedom of Information Act 1982*, Australian Government Publishing Service, Canberra, 1995.

However, in March 1997 the Prime Minister announced that so as not to further increase the regulatory burden and compliance costs for business, the Commonwealth would not be implementing privacy legislation for the private sector.[84] In order to avoid a patchwork of regimes, the Prime Minister also requested the states and territories not to separately legislate for privacy in the private sector. The Northern Territory and Queensland agreed to this request.

Instead, the Prime Minister offered the services of the federal Privacy Commissioner, currently Ms Moira Scollay, to assist business develop voluntary codes of conduct to meet privacy standards.

As a result, in August 1997 the federal Privacy Commissioner released a consultation paper titled *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector*. The self-regulatory scheme proposed in the paper, which deals with the fair and responsible handling of personal information in the private sector, clearly encompasses the calls for consistency in privacy standards across all sectors in Australia.

The Commissioner's process is discussed in more detail in chapter 10 of this report which deals with the issue of privacy in the private sector. However, it is relevant to note at this stage that as a result of consultation, the Commissioner decided to separate her process into two components; firstly, the establishment of a national set of information privacy principles and secondly, the establishment of compliance mechanisms. Given the desirability for national principles to be agreed upon before one of the current state or federal initiatives comes up with its own set of principles, the Commissioner set this task as a high priority. (These other initiatives are discussed later in this chapter.)

In February of this year the federal Attorney-General launched the results of the first stage of federal Privacy Commissioner's process, that is, the *National Principles for the Fair Handling of Personal Information*[85]. The Commissioner describes these principles as a privacy 'benchmark' for the handling of personal information by Australian businesses and has urged organisations to adopt them.

The Commissioner has also stated that she will shortly commence discussions on implementation and compliance arrangements with respect to these principles.

4.3 CURRENT PRIVACY LEGISLATION IN OTHER AUSTRALIAN STATES AND TERRITORIES

4.3.1 General assessment

Privacy regulation at the state level, beyond that covering the use of listening devices and telecommunications interception, has been sparse. However, more recently both New South Wales and, as noted above, Victoria have indicated the intention to introduce more comprehensive 'information' privacy legislation.

[84] Refer to the Prime Minister's media release concerning privacy legislation dated 21 March 1997.

[85] Federal Privacy Commissioner, February 1998.

4.3.2 New South Wales

The most significant privacy legislation at the state level has for a long time been the New South Wales *Privacy Committee Act 1975*.[86] This Act established the Privacy Committee of New South Wales as in effect a 'privacy ombudsman'. This Act also contains a number of features that were not adopted by the later Queensland legislation of the same name and which is described earlier in section 3.3.2 of this report. In particular, the New South Wales legislation has no sunset clause and the committee enjoys marginally more independence than its Queensland counterpart did. The New South Wales committee has also maintained quite a high profile.[87]

The New South Wales Privacy Committee is to consist of not less than 12 and not more than 15 members who are appointed by the Governor on the advice of the New South Wales government.[88] Members are required to include government and non-government parliamentarians, academics and persons with a special knowledge of, or interest in, matters affecting privacy.[89]

The functions of the committee as set out in the Act include:

- conducting research and collating information in respect of any matter relating to the privacy of persons;
- making reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interests of privacy of persons;
- receiving and investigating complaints about alleged violations of the privacy of persons (in this respect, the committee may make reports to complainants)[90];
- in relation to the privacy of persons: disseminating information; undertaking educational work; and making public statements; and
- conducting such inquiries and making such investigations as its sees fit.[91]

In order to carry out these functions, the Committee is conferred the power to require any person to give or produce to a member of the committee any statement of information, any document or thing or a copy of any document.[92] In addition, in relation to any inquiry or investigation conducted by it, the Committee has the powers, authorities, protections and immunities conferred on a commissioner by Division 1 of Part 11 of the *Royal Commissions Act 1923*. That Act also applies to any witness summoned by or appearing before the Committee in the same way as it applies to a witness summoned before a commissioner.[93]

---

86 The New South Wales legislation largely embodies recommendations made in the 1973 'Morison Report' on the law of privacy. Refer to section 2.3 of this report.

87 Tucker, op cit, p 71.

88 s 5(1)-(3). One member is to be the Executive Member of the Committee.

89 s 5(4).

90 The Queensland Privacy Committee could not report to complainants. Refer to the discussion at section 3.3.2 of this report.

91 s 15.

92 s 16.

93 s 16(2).

Thus, the New South Wales Privacy Committee may be said to be an advisory and investigatory body in relation to privacy issues in New South Wales. However, in contrast to the *Privacy Act* (Cth), the New South Wales legislation does not set down any information privacy principles to be adhered to by the public (or private) sector.

The need for comprehensive data protection (information privacy) legislation has long been realised by the New South Wales Privacy Committee,[94] and there have been a number of unsuccessful attempts to introduce such legislation in New South Wales. These attempts have included the Privacy and Data Protection Bill 1994 which was referred to a Select Committee but lapsed on the prorogation of the 50th Parliament, and the re-introduction of that bill as a Private Member's Bill in 1995.

In 1995, the New South Wales Attorney-General and Minister for Industrial Relations, Hon J W Shaw MLC, foreshadowed the introduction of comprehensive privacy legislation incorporating a New South Wales Privacy Commissioner with wide powers to receive, investigate and conciliate complaints including powers of sanction. The Commissioner was reportedly to be supported by a privacy advisory committee and merged with the New South Wales Anti-Discrimination Board to form a new Human Rights and Justice Commission. This legislation was apparently not only going to set out IPPs to apply to the state public sector but also apply those principles to the private sector via industry codes of practice.[95]

Despite these announcements, the New South Wales government has yet to introduce comprehensive privacy legislation into its Parliament. However, in October 1997 the New South Wales Attorney-General confirmed the government's intention to introduce privacy legislation in the near future stating that the proposed information protection principles to be enshrined in that legislation will apply to the state's public sector soon after the legislation is passed. The Attorney-General further stated that in order to ensure consistency these principles will be similar to the IPPs contained in the *Privacy Act* (Cth).[96]

The New South Wales Attorney-General also confirmed that the proposed legislation will establish a statutory office of Privacy Commissioner which, for administrative efficiency, will be merged with the Anti-Discrimination Board to form a new body. The Privacy Commissioner will investigate and conciliate complaints concerning breaches of the principles. Should this process fail then a complainant will have the ability to bring an action for damages in the District Court.[97]

This latest announcement did however indicate that New South Wales' proposals for regulation of privacy in the private sector have changed from that reported earlier. This is no doubt partly due to developments in this regard at the Commonwealth level. It would seem from the Attorney-General's comments made in 1997 that the proposed Privacy Commissioner will have the existing functions of the Privacy Committee for the private sector and be able to receive, investigate and conciliate complaints about breaches of privacy generally.[98]

---

94 See the New South Wales Privacy Committee's submission to the Select Committee on the Privacy and Data Protection Bill 1994, July 1994.

95 See G Griffith, *Privacy and Data Protection Law Reform: Some Relevant Issues*, Briefing Paper no 15/96, New South Wales Parliamentary Library Research Service, June 1996, pp 4-7.

96 Paper given by the Hon J Shaw, MLC at the 1997 Australian Privacy Summit, Sydney, 21 October 1997.

97 Ibid.

98 Ibid.

4.3.3 Victoria

In 1996 Victoria's Treasurer and Minister for Multimedia, the Hon Alan Stockdale MLA, announced the establishment of the Data Protection Advisory Council (DPAC) to inquire into, consider and report to the Minister on the most appropriate regulatory regime for Victoria governing collection, storage and transfer of information, particularly personal information held by public sector organisations. In addition, the DPAC was to 'consider the desirability of regulation covering the private sector in light of the Commonwealth Government's [then] activity in the area'.[99]

At the time of establishing the DPAC, the Minister stressed the importance of its work in light of the government's *Victoria 21 Policy* which, in part, aims to ensure the electronic delivery of a number of government services by the year 2000. The key to the success of this electronic service delivery (ESD) was recognised by the Minister to depend on the trust held by Victorians that information they provided to the government would not be misused or accessed by unauthorised persons.[100]

The DPAC reported to the Minister on 20 December 1996 and whilst that report has not been publicly released, the Chairman of the Council, Mr Victor Perton MP, has stated that in general the Council recommended state data protection legislation to apply to Victoria's public sector. In terms of the private sector, the Council advised that, as far as possible, the private sector regime should be achieved with maximum national uniformity.[101] In this regard the Council apparently recommended a reserve position should the Commonwealth Parliament not pass privacy legislation before July 1998.[102]

An additional advisory group, the Victorian Government Electronic Business Framework Group, was also established in 1997 to consider the facilitation of electronic commerce in the state. This group, in conjunction with the DPAC, has recommended that an Electronic Commerce Framework Act be passed dealing with matters such as electronic signatures, electronic evidence, computer crimes and mechanisms for the recognition of industry codes of conduct.

Initially it was reported that Victoria would introduce both the Electronic Commerce Framework Act and data protection legislation early in 1997.[103] However, it is understood that this move has been delayed due to the federal government's announcement that it will not be introducing privacy legislation for the private sector.

Victoria's initial response to that announcement was that it would introduce its own privacy legislation covering both the public and private sectors.[104] However, subsequent indications were that, in the interests of national consistency, the Victorian government would delay introduction of its legislation until the outcome of the federal Privacy Commissioner's consultation in relation to a national set of privacy principles. The suggestion in this regard

---

99 G Greenleaf, 'Victoria's Data Protection Advisory Council', *Privacy Law and Policy Reporter*, vol 3, 1996, p 73.

100 Ibid.

101 Perton, February 1997, op cit, p 15.

102 V Perton, 'Victorian Initiatives in Privacy: Data Protection and Multimedia', Paper presented at the Privacy and Data Protection Conference, Sydney, 19-20 March 1997, p 8.

103 Ibid, p 7.

104 J Riley, 'Banks fear Victoria jumping gun on privacy', *The Australian*, 7 October 1997, p 33.

was that Victoria's data protection legislation would be capable of incorporating these national principles.

As at the date of writing, the Victorian government has not introduced any privacy legislation and nor has it made any statement as to its intentions with respect to implementation of the national principles released by the federal Privacy Commissioner in February 1998 within its proposed privacy legislation.[105]

4.3.4 Other states and territories

Whilst the issue of privacy appears to be on the agenda of other Australian states and territories, none have yet introduced comprehensive privacy legislation.

However, South Australia has applied by cabinet administrative instruction a modified version of the Commonwealth IPPs to its public sector since 1 July 1989. A Privacy Committee consisting of five members was also established to complement the introduction of these IPPs. The functions of this committee include:

- advising the Minister as to the need for, or desirability of, legislation or administrative action to protect individuals' privacy;
- recommending to the government measures that should be taken to improve the protection of individuals' privacy;
- making publicly available information as to methods of protecting individuals' privacy and measures that can be taken to improve existing protection;
- monitoring the manner in which the administrative scheme of IPPs is being implemented; and
- referring complaints concerning violations of individuals' privacy to the appropriate authority.

The committee can also at any time appoint a person to investigate and report back to it with respect to an agency's compliance with the IPPs,[106] and can exempt a person or body from compliance with one or more of the IPPs. Any details of exemptions so granted must be included in the Committee's annual report.[107]

The ACT is subject to the *Privacy Act* (Cth) and has also recently passed specific legislation concerning privacy and health which applies to both its public and private sectors.[108]

4.4 PRIVACY LEGISLATION IN RELEVANT INTERNATIONAL JURISDICTIONS

In framing new information privacy laws in Australia reference is often made to the privacy regimes in New Zealand and Canada. Given that these are common law jurisdictions comparative to Queensland some brief background as to those regimes is made below.

---

105 The issue of privacy in the private sector is discussed in more detail in chapter 10.

106 See Part III of the Cabinet Administrative Instruction No 1 of 1989 (Re-issued 30 July 1992).

107 See clause 4(1) & (2) of the instruction establishing the committee dated 6 July 1989.

108 This legislation is discussed further in chapter 10 of this report.

4.4.1 New Zealand

In 1993 New Zealand enacted comprehensive privacy legislation regulating information privacy in both its public and private sectors. Prior to that, privacy protection was largely limited to that afforded by two pieces of legislation. The first of these was, and still is, the New Zealand *Bill of Rights Act 1990*. This Act contains no express right to privacy, although some privacy protection is afforded by the right against unreasonable search and seizure.

The second piece of legislation was the forerunner to the 1993 Act. The *Privacy Commissioner Act 1991* (NZ) was passed following a number of attempts to enact privacy legislation. However, this Act did not implement all previous privacy proposals. It primarily established an office of Privacy Commissioner and authorised information matching by certain government agencies. An inquiry process followed with respect to whether a legally enforceable information privacy regime should apply to the private sector. This process resulted in the passing of the *Privacy Act* in 1993.[109]

The centrepiece of the *Privacy Act 1993* (NZ) is twelve information principles which regulate the collection, storage, security, use, access, disclosure and correction of 'personal information'[110] held by 'agencies'[111]. These principles are based on the OECD Guidelines and are similar to those set out in the *Privacy Act* (Cth) with the exception of an additional principle relating to the use of 'unique identifiers'.[112]

The Act also establishes a Privacy Commissioner who has a broad range of functions including receiving and investigating complaints, monitoring compliance with the legislation and commenting on the privacy implications that any proposed legislative, administrative or other action may have.[113]

Persons dissatisfied with the outcome of the Privacy Commissioner's determination in relation to a complaint have the ability to institute civil proceedings before the Complaints Review Tribunal.

In addition, the Commissioner has the ability under Part VI of the Act to issue codes of practice which modify the IPPs so as to be more suitable to specified agencies, information, activities, industries or professions. These codes are formulated as disallowable instruments and a breach of a code is treated as a breach of an IPP. Thus, the complaints and enforcement provisions in the Act still apply.

The Privacy Act also:

- gives the Privacy Commissioner certain functions in relation to monitoring the conduct of data matching by authorised public sector agencies and to report on that activity in

---

109 The history leading up to the enactment of the *Privacy Act 1993* (NZ) is detailed in Longworth and McBride, op cit, pp 17-30.

110 Personal information is defined in s 2(1) as information about an identifiable individual.

111 'Agency' is defined in s 2(1) to be 'any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector'; and, for the avoidance of doubt, includes a government department. There are also a number of exceptions to the definition which are also set out in s 2(1).

112 A 'unique identifier' is defined in s 2(1) to mean an identifier that is assigned to an individual by an agency and uniquely identifies that individual in relation to that agency. However, it does not include a person's name.

113 See s 13.

his/her annual report;[114] and

- sets out four public register principles regulating access to, and use of, personal information stored on public registers.[115]

The New Zealand Privacy Commissioner is currently conducting a complete review of the operation of the *Privacy Act* (NZ).[116]

4.4.2 Canada

Whilst the *Canadian Charter of Rights and Freedoms 1982* which forms part of Canada's Constitution does not contain an express right to privacy, it does offer individuals privacy protection in their dealing with the government through the right to be secure from unreasonable search and seizure and the right to life, liberty and security of the person. This privacy protection however most often occurs in the criminal law context.

In addition to this limited protection offered by the *Charter*, privacy is also protected in Canada by two other means.

Firstly, some Canadian provinces have passed legislation granting their residents civil protection against violations of their territorial and personal rights, that is, they have created a statutory tort of privacy.[117]

Secondly, privacy of information is protected in Canada by specific data protection legislation at both the federal and provincial levels.

Canada's federal *Privacy Act 1982* governs the collection, use, disclosure, retention and disposal of personal information by federal government agencies. Like Australia's *Privacy Act* this legislation is based on the 1980 OECD Guidelines. The federal Privacy Commissioner is charged with the responsibility of monitoring compliance with the Act and investigating complaints from individuals regarding privacy.

Many of Canada's provincial governments have also passed similar legislation regarding information privacy in the public sector.

To date Quebec is the only Canadian jurisdiction which has introduced privacy legislation to cover its private sector. Since 1994 the *Act Respecting the Protection of Personal Information in the Private Sector* has granted individuals a right of access to, and control over the dissemination of, personal information held by *private* sector businesses operating in Quebec.

Outside of Quebec attempts have been made in some sectors to introduce voluntary privacy codes detailing guidelines for personal privacy protection. Areas in which voluntary codes have been introduced include direct marketing, the banking sector and the telecommunications sector.

---

114 See Part X of the Act. Current authorised data matching programs are designed to detect overpayments of social benefits.

115 See Part VII of the Act. These public register privacy principles are discussed further in section 6.4 of this report.

116 This review is in accordance with s 26 of the *Privacy Act 1993* (NZ).

117 The operation of these statutory torts is discussed further in chapter 5 of this report.

In 1996 the Canadian Standards Association also released its *Model Code for the Protection of Personal Information* which contains ten principles for all organisations which collect or use personal information. The Model Code is designed as a standard which could be certified and registered like other quality management standards. Thus, companies which comply with the Model Code could become privacy standard accredited.[118]

There have been suggestions that the Canadian *Model Code* may form the basis of an international standard, and could perhaps satisfy the European Union's 'adequacy' criteria (as set out in the EU Directive). Australia's federal Privacy Commissioner participated in a meeting of the International Standards Organisation in May 1997 which discussed this possibility.[119]

The Canadian federal government has now decided that, for a range of reasons, it can no longer rely on a self-regulatory approach to privacy protection in the private sector. It has announced that by the year 2000 Canada aims to have federal legislation providing effective and enforceable protection of privacy rights in the private sector. In January 1998, a joint Justice and Industry Ministries Task Force issued a discussion paper about the form that the legislation should take.[120] The paper acknowledges the work done on the Model Code as a valuable foundation, but states that light, flexible and effective legislation will provide the kind of backup that is needed to ensure that, when there are problems, consumers have mechanisms for recourse.

---

118 C J Bennett, 'Adequate Data Protection by the year 2000: The Prospects for Privacy in Canada', *International Review of Law, Computers & Technology*, vol 11 no 1, 1997, pp 79-92.

119 Federal Privacy Commissioner's *Ninth Annual Report*, op cit, p 41. It does seem now increasingly unlikely that voluntary codes will suffice. See the further discussion on this in chapter 10 of this report.

120 Industry Canada and Justice Canada Task Force on Electronic Commerce, 'The Protection of Personal Information - Building Canada's Information Economy and Society' January 1998, see http://canada.justice.gc.ca

5. CHAPTER 5 - A PRIVACY FRAMEWORK FOR QUEENSLAND

5.1 INTRODUCTION

In chapter 3 the committee recommended that the Queensland government introduce measures to ensure the greater protection of individuals' privacy. In particular, the committee recommended that the privacy protection of personal information held by state government departments and agencies be addressed as a matter of priority.

In this chapter the committee canvasses a number of options which may be employed in Queensland in order to address these priority concerns. In undertaking this assessment and drawing conclusions as to the viability of the various options, the committee has formed a privacy framework for Queensland.

The committee believes that given the paucity of Queensland's privacy laws, the establishment of a privacy framework is important. Foremost this framework should, in accordance with the committee's recommendations noted above, address information privacy in the state's public sector. However, importantly it should also serve as the structure within which other privacy concerns can be addressed.

5.2 PRIVACY PROTECTION OPTIONS

There are a number of ways in which the privacy of information about individuals held in Queensland's public sector may be further protected. The previous discussion in chapters 2 and 3 reveal that the three most readily identifiable and plausible of these options which may be considered either in isolation or combination are:

- a statutory tort of privacy;
- information privacy principles (implemented either by statute or administratively); and/or
- a privacy commissioner or privacy committee.

Arguably 'self-regulation' is also an option with respect to privacy regulation in the public sector. However, as the submissions from departments themselves recognise, the current situation (which is in effect self-regulation) is less than ideal because the absence of state legislation makes it difficult to develop and enforce consistent policies concerning the privacy of information.[121]

The committee canvasses in this chapter each of the above options and their suitability for Queensland either alone or in combination with another option. Considerations which the committee believes are important in making this assessment are that any form of privacy regulation for Queensland should have at least the following aspects:

- it should be practicable and workable;

[121] Refer, for example, to the submissions noted in chapter 3. Self-regulation via industry codes of conduct in the context of the private sector is discussed in more detail in chapter 10 of this report.

- the costs of any regulatory scheme should not outweigh the scheme's benefits;
- it should be adaptable enough to suit all state government departments and entities; and
- it should be able to keep up to date with privacy issues emerging from new technologies.

Another important consideration for the committee has been the fact that the demarcation between the public and private sectors is becoming increasingly blurred. This is due to the commercialisation, corporatisation and the contracting out of services traditionally provided by the government. Given the ensuing difficulty in some cases in determining whether an entity is public or private there are strong arguments for consistency as far as possible in standards required of each. Where appropriate, the committee refers to the impact of this observation throughout the following chapters.

In drawing conclusions as to the appropriateness of each/a combination of the above options the committee has been mindful of all of the above considerations.

5.3 A STATUTORY TORT OF PRIVACY

5.3.1 Background

As noted earlier, the common law in some jurisdictions such as the US recognises a tort of privacy. Other jurisdictions have, or have attempted to, create torts of privacy by statute (legislation).

A statutory tort in effect grants persons the right to bring an action, usually for damages, against someone who they allege has infringed their privacy. Legislation creating such a tort can also define aspects of it such as the scope of the right, exemptions, defences and remedies whether damages or otherwise.[122]

The committee has researched with interest the existence and operation of statutory torts of privacy in other jurisdictions. For example, statutory torts of privacy have been in existence for some time in the Canadian provinces of British Columbia (pursuant to the *Privacy Act 1968*) and Manitoba (pursuant to the *Privacy Act 1970*).

These statutes confer on citizens a general 'right to privacy' (which is subject to the courts' interpretation) and set out general defences. However, despite the length of time that these statutes have been in force, there are very few reported decisions.

There have also been a number of attempts to introduce statutory torts into the UK and various Australian jurisdictions, although to date all have been unsuccessful.[123] These attempts include the:

- Right of Privacy Bill 1969 (UK);

---

122 See generally: A Samuels, 'Privacy: Statutorily Definable?', *Statute Law Review*, vol 17, no 2 1996, pp 115-127.

123 The submission received from the Department of Justice canvasses these earlier attempts at p 7.

- Privacy Bill 1974 (SA);
- Privacy Bill 1974 (Tas);
- the Human Rights Bill 1973 (Cth); and
- the Privacy Bill 1990 (SA).[124]

The 1969 UK Right of Privacy Bill was introduced as a Private Members' Bill and set out a wide definition of the 'right to privacy' which then was limited by the defences also contained in the Bill. The Bill was withdrawn following criticism that it would unduly hamper freedom of speech and of the press, and the announcement that a review of the law of privacy would be undertaken (which resulted in the *Younger Committee* Report).[125]

The two 1974 state bills similarly contained definitions of privacy and established a tort for violation of privacy. Proof of damage was not necessary to commence an action. Both proposals created considerable comment and criticism, particularly from the media who believed it would unduly hamper them.[126]

The Human Rights Bill 1973 (Cth) represented a much more limited attempt at protecting privacy. The Bill merely provided that 'an unreasonable search or seizure is an unlawful interference with privacy'.[127]

The subsequent South Australian Privacy Bill of 1990 also created a broad right to privacy which could be actioned without proof of damages and set out defences, remedies and exemptions. The Bill was considered and approved by a Select Committee of Privacy but has yet to be passed by the South Australian Parliament.

What is evident from research as to these existing and proposed statutory torts is that a statutory tort of privacy could have a number of advantages including the following.

- A statutory tort has the ability to operate in all areas in which privacy concerns arise including those which may arise in the future. Therefore, a tort could operate beyond just information privacy and extend to territorial, personal and communications privacy.
- A statutory tort could also apply to both the public and private sectors.
- A statutory tort could, depending on it formulation, operate to give a remedy to everyone who could substantiate an allegation of a privacy intrusion.
- A statutory tort would fulfil Australia's obligations under international covenants such as the ICCPR (although it would not satisfy the terms of the EU Directive).
- A statutory tort would give specific legislative recognition of the right to privacy which in turn would have an educative effect in the community.

---

124 For discussion on the first four of these bills see generally ALRC, 1983, op cit, vol 2, pp 21-23 and Tucker, op cit, p 72.

125 ALRC, 1983, op cit, p 22, para 1077.

126 Ibid, p 22, para 1076.

127 Ibid.

However, the committee's research has also revealed many disadvantages of a statutory tort. These include the following.

- It would be difficult to define the concept of privacy in a statute as privacy is 'inherently vague and uncertain and imprecise'.[128] This could result in some areas of privacy not being adequately protected.

- The law could be used to prevent legitimate publication by virtue of 'gagging' writs.[129] In other words, the tort could possibly be used so as to have an adverse impact on the freedom of speech, communication and the press.

- The costs associated with enforcing a right under a statutory tort would be high and may make the remedy illusory to the ordinary citizen.

- Relying on the courts to enforce one's right to privacy will, most likely, result in substantial delay in remedying a breach.

- The remedies defined in the legislation, such as damages and injunctions, may not be appropriate to all privacy intrusions.

- The fact that the law would develop as matters were brought before the courts would mean that it was a more reactive as opposed to a pro-active approach to privacy issues. This would inevitably result in delays in the law meeting technology.

- As principles would be decided largely on a case by case basis, a lack of clear and definite privacy standards would result. (Although admittedly the right to privacy as a principle would remain.)

- A tort alone would not provide for a dedicated and continual monitoring body for privacy issues.[130]

The majority in the UK *Younger Committee* Report (1972), and Professor Morrison in his 1973 report to the Standing Committee of the Commonwealth and State Attorneys-General, recommended against the creation of a statutory tort of privacy.

Likewise, the ALRC in its 1983 report on privacy also considered the operation of a statutory tort and concluded:

> *The Commission is not persuaded that it is appropriate to create a general tort of 'invasion of privacy'. Such a tort would be too vague and nebulous. It would need to be worked out, case by case, as courts and administrative tribunals grappled with particular fact situations that come before them. In time, perhaps, a set of principles might be developed through this process. The limits of the tort would ultimately be fixed. How it would affect freedom of the press, of speech and of information would only then be clear. There is an additional reason why this approach is unsatisfactory. It might encourage the view that the enactment of such a law is all that is necessary for the effective protection of privacy. This would be an illusion. However important*

128 Samuels, op cit, p 116.

129 Ibid, pp 115-116.

130 These advantages and disadvantages are canvassed in the ALRC's 1983 report, op cit, vol 2, pp 23-24 and D Yarrow, 'Developments in the Law of Privacy - Law and Policy', *Queensland Lawyer*, vol 17, 1996, pp 60-66, p 64.

> *they may be as statements of legal rights and duties, general tort remedies are not always available, in practice, to those who need them most. They are not a substitute for comprehensive measures for the protection of privacy such as are recommended in this report. The Commission has concluded that a general tort of 'interference with privacy' would be undesirable at this stage.*[131]

5.3.2 Arguments raised in public consultation

Only a small number of the submissions received by the committee specifically canvassed the issue of a statutory tort of privacy. There was little support for the creation of such a tort in these submissions. Two submissions which did support the creation of such a tort also recommended that it be appropriately limited and combined with some other form of privacy protection. These submissions were received from the Queensland Council for Civil Liberties (QCCL) and the Townsville Community Legal Service Inc (TCLS).

The QCCL stated that it considers:

> *…the creation of a statutory tort of privacy, with appropriate protections to balance both the interests of the individual and issues related to freedom of the press, together with the possible introduction of a criminal offence of privacy intrusion, would perform a significant role with respect to the protection of the privacy of individuals.*[132]

Similarly, the TCLS submitted that like the *Anti-Discrimination Act*, certain types of behaviour or conduct could be made unlawful with recourse to civil remedies for breaches of privacy by such conduct or behaviour. However, the TCLS also recognised that there would need to be clear definitions and exemptions to a statutory tort to take account of countervailing considerations such as freedom of speech and protection of the public.

5.3.3 Analysis and conclusion

During its recent study tour to Canada, the committee canvassed with a number of bodies the operation of the provincial statutory torts of privacy.[133] The committee observed that given the amount of time these torts have been in existence, there have been relatively few reported decisions concerning attempts to enforce rights pursuant to them. Although this may to a small extent be explained in the case of jurisdictions which have both statutory torts and legislation covering the protection of information privacy in the public sector, the committee also queried whether it reflected the lack of utility of statutory torts due to time, cost, access and general awareness of the right.[134]

A comment in a paper provided to the committee during its study tour summed up the evidence the committee received regarding these statutory torts:

> *These laws generally permit individuals to claim tort damages against others in the*

---

131 ALRC, 1983, op cit, vol 2, p 24, para 1081.

132 Queensland Council for Civil Liberties, submission dated 12 August 1997, p 6.

133 British Columbia, Saskatchewan, Manitoba and Newfoundland have all enacted statutory torts.

134 See also D Kratchanov, 'Personal Information and the Protection of Privacy', Paper appended to the proceedings of the 1995 meeting of The Uniform Law Conference of Canada. In this paper the author also notes that the provincial Acts establishing tort liability for invasion of privacy have not generated much judicial consideration and have been difficult to enforce.

> *private sector who violate their privacy. A person might, for example, claim damages if a private investigator or employer conducts surveillance of the person's residence, vehicles or personal activities. However, these statutes are seldom used. Moreover, they do not apply to governments who invade the privacy of their citizens. Canadians in general also lack a common law (judge-made) tort to protect them against invasions of privacy*.[135]

Based on this experience and for many of the reasons noted above, the committee believes that a statutory tort *alone* would prove an ineffective means of addressing privacy concerns in the public (and private) sector. In particular, the committee is concerned that a statutory tort:

- must be enforced in the courts which is expensive both in terms of time and financial cost;
- does not represent a clear, explicit and comprehensive statement as to what is good privacy practice; and
- by virtue of being reactive in nature, privacy principles associated with the tort will develop slowly and on a case by case basis which is unacceptable in the age of rapidly advancing technology.

A statutory tort alone would also not provide for a privacy advocate and/or guardian.

Moreover, the committee is concerned that such a tort, even if *combined* with other forms of privacy protection, could have an adverse impact on the freedom of speech, communication and the press. A real possibility would exist that legal action pursuant to the tort could be used as a means of preventing legitimate publications.

5.3.4 Recommendation

Recommendation 2 - The committee does not recommend that a statutory tort of privacy be created in Queensland.

5.4 INFORMATION PRIVACY PRINCIPLES

5.4.1 Background

As discussed in chapter 2, the OECD Guidelines have acted as an international precedent for information privacy principles (IPPs). The eight information privacy principles set out in these guidelines are applicable to both the public and private sectors and have been adopted in one form or another in the privacy legislation of many industrialised countries.

In effect, the OECD Guidelines set out what constitutes good privacy practice in relation to ensuring the privacy of 'personal information'. (Personal information is generally described as information about an identifiable individual.)[136]

---

135 The Privacy Commissioner of Canada, A submission to the Special Joint Committee on a Renewed Canada 'Entrenching a Constitutional Privacy Protection for Canadians' dated 3 December 1991, p 8.

136 In section 6.6.2 the committee discusses further whether 'personal information' is an appropriate definition to be used in proposed Queensland privacy legislation.

Thus, as seen in the case of the *Privacy Act 1988* (Cth) a well-drafted, broad set of IPPs can govern standards for matters such as collection, storage, access, use and disclosure of 'personal information' by government entities or 'agencies' as they are defined in that Act.[137]

Arguments for the introduction of IPPs include the fact that they:

- are flexible in that the principles can be periodically reviewed and updated to cover emerging privacy issues;
- are adaptable in that they can be tailored (for example, by codes of practice) to meet specific industries, activities or professions;
- constitute an explicit and certain statement as to what is good privacy protection;
- represent what constitutes 'best practice' in terms of protecting information privacy; and
- can be extended to apply beyond the public sector to the private sector (as is the case under the *Privacy Act* (NZ)).

It is also possible that the IPP model can be expanded upon so that the privacy principles do not relate solely to information privacy. This potential is demonstrated by the Australian Privacy Charter which was released by the Australian Privacy Charter Council in December 1994.[138]

The Australian Privacy Charter contains 18 general principles designed to encompass and apply to all forms of privacy and surveillance and both private and public sector users and clients. Thus, whilst the Council recognises that information privacy remains the prominent concern in privacy protection, its Charter addresses privacy issues which are emerging from enhanced surveillance technology.[139]

Arguments against the introduction of IPPs include the fact that:

- they could constrain the exchange of data which is in the public interest (For example, some data matching or exchange programs bring about time and cost efficiencies. In other cases the exchange of information may operate to prevent fraud, or be necessary for legitimate needs of business.); and
- the cost of implementing IPPs could outweigh their benefit.

Forseeably costs associated with the implementation of IPPs could include those associated with: implementing new systems, policies and practices (both computerised and manual) in

---

137 The committee also uses the terms 'agency' in this report to refer to state government departments, statutory authorities and other state public sector entities. In chapter 8 of this report the committee discusses whether this definition should be extended to include local governments, government owned corporations and service-providers who have been contracted by the government to perform services which would otherwise be provided by the government.

138 The Australian Privacy Charter Council is a group of citizens representing the business, academic, legal, information technology, and health communities, consumer and privacy advocates, the media and politicians. It was formed in 1992 under the chairmanship of Justice Kirby AC, CMG, then President of the New South Wales Court of Appeal, to develop a privacy charter. The draft Australian Privacy Charter which was circulated widely nationally and internationally for comment was launched on 5 December 1994.

139 The Charter is discussed again in chapter 11.

relation to both storage and access to information; handling complaints about privacy; conducting periodic audits to ensure compliance with the IPPs; reviewing and therefore perhaps reprinting forms used to obtain information; and training staff with respect to the IPPs and compliance with them.

5.4.2 Arguments raised in public consultation

Those submissions which addressed the way in which privacy could be protected in the state's public sector strongly supported the implementation of a set of IPPs. These submissions came from a broad cross-section of the community including government departments and agencies, private citizens, community legal and advocacy groups, local authorities, and various bodies within the health industry.

Submissions varied on the issue of the cost of implementing IPPs applicable to government departments and agencies. Some submitters stated that they were not qualified to comment. Others did not perceive cost as a significant issue particularly when weighed against the benefits of implementing IPPs.

Government departments also gave varied responses on the issue of the cost to them of complying with IPPs, although one would expect compliance costs to vary from department to department depending on the amount of personal information collected by them.

On the one hand a number of departments made comments such as the following.

> *It is unlikely that the cost would outweigh the public benefit. After the initial implementation cost, on-going costs to agencies should be minimal.* (Department of Training and Industrial Relations)[140]

> *While the initial cost of establishing the IPPs would be significant, these costs would lessen once the IPPs became part of management systems within agencies.* (Joint submission from Main Roads and Queensland Transport)[141]

> *No. [To the question whether the costs associated with IPPs would outweigh the public benefit flowing from their implementation.] Privacy is an important value to uphold and protect.* (Department of Public Works and Housing)[142]

On the other hand, some government departments advised the committee that the costs associated with implementing IPPs could be substantial and that a phased-in approach would operate to reduce this cost.

In this regard the Department of Justice submitted that information privacy be protected in Queensland, to the extent that it applies to the public sector, by a three-staged approach.

- Stage 1 - The establishment of an independent statutory Privacy Commissioner.
- Stage 2 - The development of guidelines or principles and accompanying exemptions for the protection of information held by state government departments and agencies by the state Privacy Commissioner. The department proposed that these guidelines will

140 Submission dated 8 August 1997, p 2.
141 Submission, 28 July 1997, p 2.
142 Submission dated 9 September 1997, p 5.

ultimately be approved by Cabinet and issued as a Cabinet Administrative Instruction.

- Stage 3 - The administrative guidelines or principles may, at some future time, have legislative underpinning.

On this basis the department argued that any costs for departments and agencies associated with privacy implementation in Stage 2 will be minimal and should be met from within existing budgets. However, the department also stressed that this was dependent on: staged implementation of the guidelines over a number of years (which would mean that, for example, as computer systems are updated the guidelines will be followed in making those changes); the guidelines being implemented only as guidelines for which there was no sanction for non-compliance; and the guidelines being based on the OECD Guidelines but tailored to suit Queensland government needs.

The Department of Families, Youth and Community Care also pointed out to the committee that there are costs associated with the introduction of a privacy regime involving IPPs and that a proper balance needs to be achieved between the ideal system and one which "reflects contemporary economic constraints and consequent priorities for resource allocation". On this basis the department also submitted that the implementation of an administrative regime as a first stage prior to the introduction of an enforceable legislative regime will reduce costs.

Mr Brett Mason from the Faculty of Law at the Queensland University of Technology (QUT) likewise recognised that the issue of cost may make administrative guidelines applicable to the state public sector more attractive at least initially and that at a later date legislation incorporating IPPs could be introduced and extended to the private sector.

The federal Privacy Commissioner stated that costs would not outweigh the public benefit flowing from the implementation of IPPs provided they were sensibly implemented. However, unlike the above submissions, the Commissioner did not see that their introduction by an administrative scheme initially was necessary to bring about this result.

> *Complying with IPPs may involve adjustment costs for some organisations. Forms may need to be changed, procedures revised and staff trained. Provided that there is an adequate phase-in period, so that organisations that need to change their practices can do so in the normal course of business, for example when ordering new stationery or brochures, the costs should be limited.*[143]

5.4.3 Analysis and conclusion

The committee sees a strong argument in favour of the implementation of broad IPPs in Queensland governing matters such as the collection, access, security, correction, use and disclosure of personal information held by state government departments and agencies.

A set of privacy principles would stand as an explicit statement and represent what is 'best practice' as far as good privacy protection is concerned. This is important from both the client and service-provider perspective. Moreover, privacy principles would assist in developing or, in some cases, reinforcing a privacy culture both within agencies and the community in general.

[143] Submission dated 26 August 1997, p 8.

Provision could also be made in the scheme within which these IPPs are implemented to ensure that they can be adapted to suit specific agencies if need be.[144]

Two particular arguments against the implementation of IPPs are noted above.

The first of these concerns the fact that IPPs could constrain the legitimate exchange of data. As noted at the outset of this report, the protection of privacy requires the careful balancing of a number of rights and interests. Indeed, the committee recognises that there may well be circumstances in which the public interest in not complying with an IPP outweighs compliance with that IPP.

However, provision to cater for this greater public interest can be built into a regime which incorporates IPPs. Both the *Privacy Act* (Cth) and the *Privacy Act* (NZ) contain procedures whereby 'public interest' exemptions from compliance with IPPs can be granted. Certain exceptions are also contained in the IPPs themselves. Therefore, the committee is not swayed by this argument provided that such measures form part of the overall privacy scheme.[145]

The second main argument against IPPs concerns cost and resource allocation. The committee recognises that the implementation costs of IPPs will vary from agency to agency according to the amount of personal information each collects. For example, departments such as Health, Education, Treasury, Families, Youth and Community Care and Transport would hold more personal information than other departments, and therefore may incur greater implementation costs.

However, the committee expects that such departments (as indeed all departments) as holders of significant amounts of personal information should already, as a matter of best practice, have in place procedures and mechanisms to ensure that personal information held about members of the community not misused. The implementation of broad IPPs should therefore to a large extent reinforce many of the guidelines currently in operation.

In fact, the submission from the Department of Justice recognises this point.

> *Many departments have already been following these [privacy] principles and have privacy protection mechanisms in place. For them little change will be required. …*
>
> *Transport has already developed several model draft policies on the basis of the Commonwealth privacy guidelines, governing access to and the release of information on:*
>
> - *Drivers' licences*
> - *Local Government parking notices*
> - *Motor vehicle registrations.*
>
> *It is understood that Transport would be very close to 100% compliance with the Commonwealth guidelines within a very short time period.*
>
> *Other departments and agencies already follow best practice procedures. This contemporary management practice demands the requisite standards of information privacy protection be observed by public sector agencies as part of the application of*

144 The modification of IPPs by codes of practice is discussed further in section 6.3 of this report.

145 The committee discusses the issue of exceptions in more detail in section 6.4 of this report.

best practice principles.[146]

As noted by the federal Privacy Commissioner an adequate phase-in period should also reduce costs. Whether this phase-in period should be in the form of an administrative scheme initially followed by a legislative scheme is addressed in more detail in chapter 6. However, as is evident from the federal Privacy Commissioner's submission, an administrative scheme at the outset is not necessary if the IPPs are phased-in.

The committee recognises the concerns regarding the cost of IPPs particularly if they are implemented immediately. However, as will become evident from discussion later in this report, the committee does believe that these concerns are addressed in particular by two factors. Firstly, the application of the various principles (that is, determining which principles should apply to information collected before, and after, the commencement of the regime) should allay some of these concerns. This is addressed later in section 6.5 of this report.

Secondly, the committee believes that any IPPs to be introduced should be cast in relatively broad terms. (This is the case with both the OECD Guidelines and the IPPs in the Commonwealth *Privacy Act*). Such principles will therefore provide the person/body responsible for enforcing the regime with some scope to exercise discretion in enforcement in the early stage of the IPP's implementation.[147]

Therefore, it would only seem to be in some residual areas that there may be both cost and administrative difficulties with the immediate implementation and enforcement of the principles. To ensure that a sensible approach is taken in this residual area, the committee does believe that there should be a phase-in period. This period will allow for agencies to change their administrative practices, and also give them time in which to conduct training and awareness programs, alter existing polices and procedures, and prepare applications for any exemptions which may seem necessary.[148]

However, the committee does believe that there must be a finite limit on any phase-in period. To extend the period beyond what is 'reasonable' will render the implementation of the principles ineffective. Considering the above matters which agencies will have to attend to, the committee believes that a period of 6 to 12 months is a reasonable period of time during which agencies can progressively change their practices to comply with the principles.

The above discussion also demonstrates that the introduction of IPPs means that other factors will have to be considered. The most significant of these factors include:

- what the IPPs should provide;
- whether the IPPs should be implemented administratively or whether they should be enshrined in legislation;
- whether provision should be made for the modification of the IPPs;
- what, if any, exceptions should apply to the IPPs;

146 Department of Justice, submission dated July 1997, pp 27-28.

147 The actual 'language' of the IPPs is discussed further in section 6.1 of this report and the person/body responsible for their implementation is discussed in the next section of this chapter and in chapter 7.

148 Refer to section 6.4 of this report as to exceptions to the IPPs.

- to what extent the IPPs should operate in respect of information already held; and
- how the IPPs should interrelate with other legislation providing access to information.

These matters are discussed in some detail in the next chapter of this report.

5.4.4 Recommendation

Recommendation 3 - The committee recommends that the first element of a privacy regime in Queensland be the implementation of a consistent set of information privacy principles (IPPs) relating to personal information collected and held by Queensland government departments and agencies.[149]

The committee further recommends that the implementation of these IPPs should be phased-in over a period not exceeding one year.

5.5 THE ESTABLISHMENT OF A PRIVACY COMMISSIONER/PRIVACY COMMITTEE

5.5.1 Background

The introduction of potentially privacy-intrusive technologies, often by powerful interests such as state government agencies has, especially since the demise of the former Queensland Privacy Committee, largely gone unchallenged. This is due to the absence of a strong and effective privacy advocate and/or some other means of privacy regulation in Queensland. Any opposition to such technologies has fallen to small public advocacy or community groups comprised of concerned citizens.

In its 1983 report, the ALRC noted the following in the context of the number of modern developments, in both the public and private sectors, that interfere with privacy.

> *These developments have been sponsored by powerful public and private sector groups in a wide variety of areas, for example, banking, insurance, law enforcement, and health and welfare administration. While these interests have been powerful and well organised, there has been no institutional advocate of privacy interests. The result has tended to be that, when decisions are being made about a new information system or a new form of intrusive conduct, the advantages of the proposal from the point of view of increased efficiency to areas such as health administration and law enforcement are fully considered. The extent to which the proposal may interfere with privacy, on the other hand, is not. That is not to suggest that privacy interests have been ignored entirely. But they have been under-represented. Institutional arrangements need to be made to redress this imbalance*.[150]

The need for an institutional privacy advocate and/or guardian is arguably heightened where individuals' privacy is infringed in the context of information which those persons are obliged to provide to the government. In that situation proponents of a privacy 'watchdog' argue that there is a clear need for an independent party to weigh the various competing interests; namely, those of the data subjects, data users and society in general.

---

149 In chapter 8 of this report the committee makes further recommendations about extending the scope of this regime to local governments, contractors and GOCs.

150 ALRC, 1983, vol 2, op cit, p 7, para 1039.

The ALRC's recommendations noted above eventually led to the establishment of a federal Privacy Commissioner under the *Privacy Act 1988* (Cth) who has developed into an integral part of the privacy regime operating at the Commonwealth level. Broadly, the essential functions of the Commissioner concern education, promoting and monitoring compliance, giving policy advice, monitoring technological trends and receiving and investigating complaints. The Commissioner is also granted powers necessary to fulfil those functions.[151]

Therefore, arguably a role exists in Queensland for a privacy advocate and/or guardian in the form of a privacy commissioner or committee. This commissioner/committee could be established in conjunction with the implementation of IPPs, as occurs at the Commonwealth level, although this not necessarily be the case. For example, the New South Wales Privacy Committee has certain functions in relation to privacy yet its legislation does not contain a set of IPPs.

However, regardless of which alternative is adopted, it is clear that Queensland must establish its own privacy body. The federal Privacy Commissioner's jurisdiction does not constitutionally extend to the states. A separate Queensland privacy committee/commissioner would have to be established to have jurisdiction in relation to Queensland's public sector.

The major argument against the establishment of such a committee or commissioner would appear to be cost.

The funds expended in support of the federal Privacy Commissioner's functions are currently part of a single annual allocation to the Human Rights and Equal Opportunity Commission. By way of guidance, the final net allocation to the federal privacy program for 1996/97 was $2 364 000.[152] Program expenditure for the financial year comprised $1 951 000 in salaries and superannuation and $482 000 in other costs.[153]

However, the federal Privacy Commissioner's office has a usual staff level of thirty-five based in a small office in Canberra and the main office in Sydney. Any similar office in Queensland would obviously operate on a much smaller scale and therefore costs would be much lower. By way of comparison the New South Wales Privacy Committee was allocated $552 100 in 1994/95 and expended $511 139. The committee is supported by a full-time secretariat of six officers who investigate complaints, undertake research and provide advice and reports on privacy issues.[154]

5.5.2 Arguments raised in public consultation

Submissions to the committee clearly supported the establishment of either a state privacy committee or commissioner primarily in conjunction with the implementation of IPPs. (The issue of whether this office should be in the form of either a committee or commissioner is discussed later in chapter 7.)

---

151 These functions and powers are described in more detail in chapter 7 of this report.

152 This amount included: $66 000 generated from publication sales, speaking fees and other minor receipts; $264 000 received from the Commonwealth Department of Social Security for data-matching regulation; and $65 000 received from the Attorney-General's Department of the ACT for monitoring and advising on the application of the *Privacy Act* to the ACT.

153 Federal Privacy Commissioner's *Ninth Annual Report*, op cit, p 113.

154 Privacy Committee of New South Wales, *Annual Report*, 1994/95, pp 54-55.

Moreover, the costs associated with the establishment of a privacy commissioner were largely seen to be far outweighed by the benefit of having a body performing the broad functions outlined above.

The Department of Justice which recommended that an Office of Privacy Commissioner be established by statute also set out in its submission a costs estimation for establishing and running an Office of the Privacy Commissioner. The cost of such an office (including the Commissioner and up to five staff) was estimated to be $756 000 for the year of establishment and $612 500 for the following year.[155]

The department concluded as a result of this analysis that the costs associated with an office of the Privacy Commissioner would not outweigh the public benefit flowing from the establishment of such an office.

5.5.3 Analysis and conclusion

The committee agrees with the majority of the submissions that there is a need for the establishment of a state Privacy Commissioner/Committee to be charged with a number of responsibilities relating to privacy. These responsibilities at least initially should be focussed on monitoring compliance with the IPPs by Queensland government departments and agencies.

The Commonwealth experience indicates that the establishment of such a Privacy Commissioner/Committee (with similar functions to his/her Commonwealth counterpart) would be an integral element of a privacy framework for Queensland.

The committee further believes that, given the importance of having an institutional privacy guardian and/or advocate, the Queensland Privacy Commissioner/Committee should be created by statute. Thus, a Queensland 'Privacy Act' could not only establish and define the responsibilities, functions and powers of a Queensland Privacy Committee/Commissioner but also act as the institutional structure of a privacy regime for the State.

Details as to:

- whether a committee or commissioner would be more appropriate;
- what specific functions that entity should have;
- what complementary powers the entity would need in order to perform those functions; and
- the importance of the independence of the entity;

are discussed further in chapter 7 of this report.

Later in this report the committee also canvasses whether this Queensland Privacy Commissioner/Committee should have functions which extend beyond the public sector and beyond information privacy.

[155] See Attachment G to the department's submission.

5.5.4 Recommendation

Recommendation 4 - The committee recommends that a Queensland Privacy Commissioner or Committee be established by legislation, namely the Privacy Act (Qld). This Privacy Commissioner or Committee is to be the second element of a privacy regime applicable to personal information collected and held by Queensland government departments and agencies.

6. CHAPTER 6 - INFORMATION PRIVACY PRINCIPLES

6.1 WHAT SHOULD IPPS PROVIDE?

6.1.1 Background

The eleven IPPs contained in s 14 of the *Privacy Act* (Cth), which are based on the OECD Guidelines, are an obvious starting point for any consideration of what IPPs for Queensland's public sector should provide.

These eleven principles are replicated in full in Appendix C of this report. Briefly, the IPPs impose on collectors and record-keepers of personal information the obligation to:

1. collect personal information only for lawful purposes and by lawful and fair means;

2. inform persons from whom personal information is solicited as to the purpose for collection;

3. ensure the relevance, currency and completeness of personal information collected and that the means of collection is not unreasonably intrusive;

4. ensure the proper storage and security of personal information;

5. maintain records to enable persons to establish what type of information is held, why it is held and how it can be accessed;

6. allow an individual access (where lawful) to their own records;

7. ensure that records of personal information are accurate, relevant and up-to-date by making appropriate corrections;

8. ensure that personal information is accurate, up-to-date and complete before using it;

9. use personal information only for relevant purposes;

10. use personal information only for the purpose for which it was collected, subject to certain exceptions; and

11. prevent disclosure of personal information to any other person or agency, subject to certain exceptions.

The twelve IPPs contained in s 6 of the *Privacy Act* (NZ) which are applicable to both the public and private sectors are also a useful reference. These IPPs, like those contained in the *Privacy Act* (Cth), regulate the collection, storage, use and disclosure of personal information. The principles also recognise the right of an individual to access and correct personal information held about them.

The New Zealand IPPs also contain an additional principle regulating the use of unique identifiers. A 'unique identifier' is defined in the Act to mean an identifier that is assigned to an individual by an agency for the purposes of the operations of the agency and that uniquely

identifies that individual in relation to that agency. However, it does not include an individual's name.[156]

An additional reference source for determining what IPPs for Queensland's public sector should provide are the *National Principles for the Fair Handling of Personal Information* released by the federal Privacy Commissioner in February 1998.[157]

As explained earlier, these principles represent the first stage in the Commissioner's process to develop consistent information privacy standards in the private sector. The Commissioner has stated that these principles have been developed with the aim to 'devise a benchmark which is relevant and flexible in the business context without compromising core privacy standards'.[158] The second stage will be determining issues associated with the implementation of these principles. At this point in time compliance with the principles is purely voluntary and the Commissioner has stated that the principles will be reviewed in six to twelve months in the light of discussions on implementation and in response to any issues which arise in practice.[159]

The advantage of Queensland largely adopting the IPPs which appear in the *Privacy Act* (Cth) in relation to its public sector would be consistency between Commonwealth and Queensland privacy regimes. Given Australia's federal system of government this would create certainty for clients and consumers as to their privacy rights irrespective of whether they were dealing with a state or federal agency. This would also be an important issue for agencies which must comply with both federal and state legislation.

However, there are also strong reasons for consistency between privacy regimes applying to the public and private sectors based on the fact that increasingly the boundary between the private sector and public sector is becoming less distinct. This breakdown in demarcation is being brought about by the commercialisation, corporatisation, and outsourcing of services formerly provided by governments. Implementation of the National Competition Policy contributes to this situation.

The question of privacy in the private sector is canvassed more fully in chapter 10 of this report. However, suffice to say that there are compelling reasons for consistency in any privacy regimes introduced for the private sector in the various Australian jurisdictions. To implement otherwise would create administrative and cost inefficiencies for the many private organisations which operate in more than one Australian jurisdiction. The federal Privacy Commissioner stressed in her February 1998 paper that her broad consultation revealed the major issue to be the need for national consistency in privacy standards in the private sector.

Thus, if privacy regimes are to apply to both the public and private sectors, there is a strong argument for them to be nationally consistent, at least in respect of core privacy principles, but probably with mechanisms to allow these principles to be specifically tailored to meet the needs of particular organisations, industry sectors, activities etc.

The Australian Law Reform Commission (ALRC) in its submission to the Data Protection Advisory Council's inquiry (into the most appropriate regulatory regime for data protection

---

156 See s 2(1).

157 Federal Privacy Commissioner, February 1998. Refer to the discussion on the consultation process leading up to the release of these principles in section 4.2.2 and chapter 10 of this report.

158 See the Commissioner's foreword to the *National Principles for the Fair Handling of Personal Information*, February 1998.

159 Ibid.

and privacy in Victoria[160]) also recommended the introduction of a comprehensive, nationally based privacy protection regime covering both the public and private sectors which should operate uniformly across all the states, territories and the Commonwealth.[161]

The manner in which the ALRC recommended this uniformity be achieved was via the Victorian government entering into negotiations with the Commonwealth and other states and territories for the introduction of a uniform privacy protection regime. It further considered that after broad agreement was sought among the various governments on the need to establish uniform privacy protection, the substantive privacy law issues should be canvassed at a meeting of the Standing Committee of Attorneys-General at the earliest possible convenience.[162]

The ALRC did however go on to recognise that the achievement of uniform privacy protection will be an involved and lengthy process, and that the Victorian government should introduce a privacy protection regime for public sector organisations as a bare minimum and as a matter of urgency. Further, in light of the desirability of a uniform approach, the ALRC also recommended that Victoria's privacy regime should be modelled on the *Privacy Act 1988* (Cth) with certain modifications in relation the contracting out of government services, public sector enterprises and the provision of services such as child care, aged care and disability services.[163]

Since the date of the ALRC's submission (October 1996) there have been significant developments regarding the issue of a privacy regime for the private sector. In particular, the federal Privacy Commissioner's current attempts to reach consensus on a national set of IPPs have already been noted.

Reference has also been made to the Victorian government's plans for introducing privacy legislation covering both its public and private sectors. Indications are that, in the interests of national consistency, particularly in the private sector, the Victorian government may adopt the national principles that were recently issued by the federal Privacy Commissioner. If Victoria takes this approach and should other states follow that lead, consistency in privacy regimes for both the private sector and the states' public sectors would ultimately result. If this was to occur it would also then appear logical for the IPPs in the *Privacy Act* (Cth) to be amended accordingly.

Unfortunately, at the date of writing, whilst the federal Privacy Commissioner has released her national principles for the fair handling of personal information, these are still at a stage where they are to be reviewed again in six to twelve months. Moreover, Victoria has not announced its intentions with respect to adopting these principles and nor has the federal Privacy Commissioner addressed implementation issues associated with them. Therefore, there are still strong arguments for Queensland to adopt IPPs mirrored on those contained in s 14 of the *Privacy Act* (Cth) at this stage.

Arguments against adopting the Commonwealth IPPs in the Privacy Act (Qld) would be that they fail to address specific 'state' concerns and, given that they were promulgated in 1988

160 Refer to section 4.3.3 of this report.
161 Submission dated 31 October 1996, p 3.
162 Ibid, p 4.
163 Ibid, pp 4-6.

and have not since been reviewed, it may be argued that they have failed to keep up with developments in technology.[164]

6.1.2 Arguments raised in public consultation

Many submissions supported consistency in privacy regimes as they apply to the public sectors of the various Australian jurisdictions and therefore recommended that Queensland should adopt, or at least model its IPPs on, the IPPs contained in the *Privacy Act* (Cth).

As the Anti-Discrimination Commission (Queensland) noted:

> *The Commonwealth Privacy Act provides a useful starting point. Consistency between State and Commonwealth legislation should be a consideration. Inconsistencies cause confusion and make legislation less accessible and user-friendly.*[165]

The University of Queensland also provided a practical example of why consistency between the Commonwealth and state privacy regimes is necessary from an agency perspective.

> *The University obtains large amounts of research grant funding from the Commonwealth agencies, and these agencies generally require the University to abide by the Commonwealth Privacy Act 1988 in respect of the activities to which the grant of funds may relate. The University would be substantially concerned if there were a conflict between the obligations imposed in the Commonwealth Act and the scope or content of any scheme for the protection of privacy proposed in the Queensland jurisdiction.*[166]

The federal Privacy Commissioner stressed in her submission the need for consistency and pointed out that whilst the IPPs which currently appear in the *Privacy Act* (Cth) primarily apply to Commonwealth and ACT government agencies, increasingly they also do or will apply to a range of private sector organisations. This includes contractors handling personal information on behalf of Commonwealth government agencies.[167]

The federal Privacy Commissioner, after referring to the various state initiatives regarding privacy legislation, also noted:

> *In this environment, it would appear hazardous for Queensland to promulgate privacy principles that depart markedly from those in the Commonwealth Privacy Act, especially in relation to the private sector. That is not to say that those principles are perfect: they have not been reviewed since their introduction in 1988 and there may be good arguments for some changes, at least at the margins. But they cover the main aspects of information privacy and the call from business for consistency of information privacy standards across jurisdictions is so strong that it is hard to see that any very different principles could be justified.*
>
> *The National Scheme process announced recently by the Privacy Commissioner provides an opportunity to reach a general consensus on a revised set of Information*

---

164 See for example the comments of Victor Perton MP, Chairman of the Victorian Data Protection Advisory Council in his paper titled, *A Privacy Act for Victoria?*, February 1997, op cit, p 15.

165 Anti-Discrimination Commission Queensland, submission dated 1 August 1997, p 3.

166 University of Queensland letter dated 25 July 1997, p 2.

167 For further discussion on developments in this regard, refer to chapter 8 of this report.

> *Privacy Principles which could be adopted in various jurisdictions.*[168]

However, some submissions considered that the Commonwealth IPPs were not an appropriate model on which IPPs for Queensland should be based.

The Australian Privacy Charter Council did not favour this approach on the basis that it considers that the *Privacy Act* (Cth) IPPs should be reviewed.

> *Commonwealth IPPs are not a satisfactory model and the OECD Principles need updating and extension. As stated, the Australian Privacy Charter Principles are designed to overcome these issues. They are designed to include protection from surveillance. They are technology neutral and will cover changes, developments and increased integration. We recommend that the Principles of the Australian Privacy Charter be used in the Queensland legislation.*[169]

Some submitters also felt that the IPPs in the *Privacy Act* (Cth) are unsuitable because they were designed for the Commonwealth and that any IPPs to apply to Queensland's public sector needed to be tailored to suit the state's particular needs. In particular, the Department of Justice and the Department of Families, Youth and Community Care (DFYCC) took this view.

The Department of Justice submitted that the development of guidelines or principles and accompanying exemptions for the protection of information held by state government departments and agencies be one of the first tasks of a Queensland Privacy Commissioner. The Department further envisaged that these guidelines be based upon standards set by the OECD but tailored to suit the needs of the Queensland government.

Later in its submission the department, whilst reiterating that a Queensland Privacy Commissioner should develop privacy guidelines, added for the purposes of 'informed discussion and debate' two options as to the content of guiding principles. The first of these options (and the department's most preferred option) represented a modification of the OECD Guidelines. The second option represented a modified version of the *Privacy Act* (Cth) IPPs.

The DFYCC also submitted that the OECD Guidelines are an ideal starting point in developing a privacy protection regime and stated that the adoption by Queensland of the *Privacy Act* (Cth) IPPs may not be appropriate given the difference in responsibilities between the state and Commonwealth governments. The department argued that state governments have greater responsibility for the provision of direct services to members of the community and therefore the intrusion of state agencies into the personal affairs of individuals is far greater than that of Commonwealth agencies.

The DFYCC used the sharing of personal information between agencies in the area of child protection as an example of an area in which there was no Commonwealth parallel. However, the department's primary concern seemed to be that there were exceptions in any IPP regime for the protection of children and persons with impaired decision-making capacity.

The committee also received evidence at its Gold Coast hearing regarding the 'blurring' of the public and private sectors. Mr Spencer from the Logan City Council commented:

---

168 Federal Privacy Commissioner, submission dated 26 August 1997, pp 6-7.

169 Australian Privacy Charter Council, submission dated 6 August 1997, p 5.

> *With the increase in and the global expansion of IT, for example, we are becoming users of the Internet and the global world of IT. We cannot see why we should have our own privacy legislation for the public sector and a different set for the private sector. We believe that with the global economy that is developing and the small world that we now operate in, there should be one set of privacy legislation on a national basis. We keep emphasising that.*[170]

6.1.3 Analysis and conclusion

The committee believes that, as far as possible, there should be consistency in privacy standards required of the Commonwealth and Queensland public sectors. The submission from the University of Queensland highlights this need from an agency perspective. Equally, clients of agencies have an interest in the same principles applying to all activities of an agency. Therefore, there are strong reasons for Queensland adopting the IPPs currently contained in s 14 of the *Privacy Act* (Cth). Consistency creates certainty, convenience and hence less cost for clients, consumers and service providers.

As noted above, some departments expressed concerns that there may be a need to modify these IPPs to suit a state, as opposed to the Commonwealth, public sector. However, the Department of Justice was not specific as to the reasons in this regard, and the DFYCC focussed on special consideration which may need to be given in relation to areas such as child protection. These areas are addressed later in sections 6.3 and 6.4 of this chapter in the context of modifications and exceptions to the application of the IPPs.

On this basis, the committee is not convinced that there are any particular 'state' considerations which would warrant departure from broad IPPs such as that which are contained in the *Privacy Act* (Cth). (Later in this chapter at section 6.6.2 the committee canvasses whether 'personal affairs information' rather than 'personal information' should be used in the context of IPPs to apply in Queensland.)

In reaching this conclusion, the committee does recognise the desirability to have national consistency in privacy protection regimes applicable to both the public and private sectors given the increasingly blurred distinction between those two sectors.[171]

The current process being undertaken by the federal Privacy Commissioner in relation to a nationally agreed-upon privacy set of IPPs (albeit currently in the context of the private sector), and the indications as to the Victorian government's intentions in this regard may well be the key towards reaching such a goal.

The 'all-round' adoption of the IPPs emanating from this process would also address arguments by some, in particular the Australian Charter Privacy Council, that the IPPs as they currently appear in the *Privacy Act* (Cth) need to be reviewed.

For example, the committee notes that the current Commonwealth IPPs do not contain an IPP concerning the use of unique identifiers similar to IPP 12 of the *Privacy Act* (NZ). The use of

---

170 Transcript, Gold Coast, 7 November 1997, p 26.

171 Later in this report the committee addresses the issue of the scope of a privacy protection regime in relation to service providers contracted by government agencies, the activities of GOCs and the private sector (see chapters 8 and 10).

unique identifiers is covered in the 1998 'National Principles' issued by the federal Privacy Commissioner.[172]

However, the committee believes that until such time as there is a clear consensus on national principles and a commitment by jurisdictions to adopt them in relation to both their public and private sectors, it is more appropriate for Queensland to model IPPs for its public sector on those currently contained in s 14 of the *Privacy Act* (Cth).

6.1.4 Recommendation

Recommendation 5 - The committee recommends that the IPPs to be implemented in respect of personal information collected and held by Queensland government departments and agencies be modelled on those contained in s 14 of the *Privacy Act 1988* (Cth).

However, the committee also recognises that given the increasingly blurred distinction between the public and private sectors, it is desirable that there be consistency between any information privacy regimes to apply to the private and public sectors. Therefore, the committee recommends that the Queensland government monitor the federal Privacy Commissioner's current process in relation to national principles for the fair handling of personal information in the private sector and the adoption of those principles by other jurisdictions. The committee believes that at some future stage the Queensland government should consider adopting the set of IPPs emanating from that process if it will achieve the goal of national consistency in information privacy regimes applicable to all Australian public and private sectors.

6.2 SHOULD IPPS BE IN GUIDELINES OR LEGISLATION?

6.2.1 Background

Given that the committee has recommended that a set of IPPs be implemented in relation to Queensland's public sector, the next issue to be determined is whether those IPPs should apply administratively (as is the case in South Australia) or by legislation (as is the case at the Commonwealth level).

If Queensland did implement its IPPs administratively then they would only apply to the public sector and would not, without more, extend to bodies to which the government has out-sourced services, or the private sector in general.

The other significant consideration in relation to whether IPPs should be implemented by legislation or by administrative means lies in their enforcement. In order to be legally enforceable by individuals IPPs will need to be enshrined in legislation.

If the IPPs were effected by administrative instruction the means of their enforcement would be primarily limited to investigations by the Ombudsman. Pursuant to s 13 of the *Parliamentary Commissioner Act 1974* (Qld) the Ombudsman has the principal function of investigating any administrative action taken by, in or on behalf of an agency. The Act also

[172] The Council's other concern in relation to covering non-information privacy concerns is a matter which the committee canvases in more detail in chapter 11 of this report.

provides the Ombudsman with certain powers in relation to conducting investigations and entitles him/her to makes reports including recommendations as a result of those investigations. A copy of such reports are also furnished to the Minister responsible for the agency concerned. Should appropriate steps not be taken within a reasonable time by the agency, then the Ombudsman may send a copy of his/her report to the Premier and cause it to be laid in the Legislative Assembly.[173]

Thus, the powers of the Ombudsman could include investigating complaints about compliance with the IPPs. However, this may require legislative amendment to the *Parliamentary Commissioner Act* to ensure complete coverage, since currently a number of bodies and persons are exempt from s 13. The Act does also not apply to a person who is a police officer in that person's capacity as a police officer.[174]

It is also possible that a breach of administrative IPPs could amount to 'official misconduct' for the purposes of the *Criminal Justice Act 1989* (Qld).[175]

6.2.2 Arguments raised in public consultation

Submissions to the committee in relation to this issue generally were in favour of IPPs having legislative underpinning. However, in particular, some departments submitted that IPPs should be implemented, at least initially, by way of administrative instruction.

The Department of Justice reasoned that the administrative introduction of privacy protection will:

- allow the scheme to be introduced rapidly;
- result in cost savings as compared with a legislative scheme because compliance costs are less in relative terms; and
- allow the government to assess the need for a legislative privacy regime at a future time.

Thus, the Department submitted that the introduction of a privacy regime for Queensland's public sector be implemented in three stages, stage two of which included the development of privacy guidelines by the Privacy Commissioner which would ultimately be approved by Cabinet and issued as a Cabinet Administrative Instruction. The advantage that the Department sees in this approach is that possible concerns and problems can be identified, assessed and dealt with in this early stage, prior to any legislative principles being implemented.

Stage three of the department's process recognises that these administrative guidelines may at some future date have legislative underpinning. However, the Department also pointed out that both New South Wales and South Australia have been in stage two for 22 and 9 years respectively which seems to indicate that the department does not necessarily consider this future date as being in the short-term.

---

173 These procedures on completion of the Ombudsman's investigations are outlined in s 24 of the Act.

174 s 12(2).

175 In its submission to the committee the CJC stated that on the basis of the current definition of 'official misconduct', a breach of a privacy principle would likely constitute 'official misconduct' and therefore fall within the CJC's jurisdiction. However, the CJC also noted that any legislation could expressly deal with that issue.

Further, the department did not believe that an administrative as opposed to legislative scheme would significantly detract from the important aim of privacy protection and stressed that compliance with its proposed scheme will be ensured through the Queensland Privacy Commissioner's powers which include the ability to receive and investigate complaints and make reports on non-compliance with the scheme in a similar fashion to the Ombudsman.

The DFYCC agreed with the Department of Justice that the cost of implementation meant it was a more realistic strategy for the IPPs to be introduced administratively initially, with the legislation representing a second phase of the process. Nevertheless, the DFYCC went on to recognise:

> *To be fully effective, privacy principles would need to be introduced through legislation. One significant factor in this regard is that without a legislative requirement there would be no obligation to review current legislation or give due consideration when enacting or drafting new legislation to ensure that adverse effects on the privacy of individuals are minimised. Furthermore an administrative scheme will not compel agencies to amend existing legislation which includes powers for the collection, use and disclosure of information.*[176]

Other departmental and government agency submissions which addressed this issue varied in their responses. However, the majority recognised that in order to be fully effective IPPs needed to be enshrined in legislation.

For example, Main Roads and Queensland Transport stated that whilst legislative-based guidelines could have difficulty in keeping up with rapid changes in technology, guidelines are more easily circumvented and do not provide any sanctions for those who breach the principles.

Submissions received from non-government organisations also reflected strong support for legislative underpinning of any IPPs to apply to Queensland's public sector in order to ensure their effectiveness. In the words of the QCCL:

> *In QCCLs' view, IPPs should be in the form of legislation. Their application should not be at the discretion of an agency, corporation or individual (which is the effect of guidelines) but should be mandatory. There should be a capacity for the use of subordinate legislation in order to rapidly respond to changing developments in technology and privacy protection. There would be a clear role for a Privacy Commissioner/Privacy Committee to advise and oversee the introduction of such subordinate legislation in response to the changing needs of privacy protection.*[177]

6.2.3 Analysis and comment

The submissions received by the committee raise some very important considerations in relation to whether IPPs should be implemented administratively or by legislation.

In general, these submissions support the legislative underpinning of a set of IPPs for Queensland's public sector, although as indicated above, some departments use cost as an argument for the implementation of IPPs by administrative instruction at least initially. However, the committee is not persuaded by the argument that the administrative

[176] Department of Families, Youth and Community Care, submission dated 12 August 1997, p 9.
[177] Queensland Council for Civil Liberties, submission dated 12 August 1997, pp 6-7.

implementation of IPPs, even if only an interim step leading to later legislation, will result in an overall significant cost saving.

Departments which currently handle personal information already should, and many do as a matter of best practice, employ and comply with privacy policies and guidelines. Comments to this effect by some departments have already been noted in chapter 3. The implementation of broad legislative IPPs should not represent a significant additional cost to those departments already employing basic best-practice guidelines in relation to the handling of personal information.

Moreover, it is difficult to see how the costs associated with the implementation of the same set of IPPs whether by legislation or administrative instruction would differ. Either the IPPs are complied with or they are not. As noted in chapter 5, the committee believes that the issue of cost is more adequately dealt with by an appropriate phase-in period as opposed to administrative implementation of the regime.

The committee further believes that the IPPs should be enshrined in legislation for the following reasons.

- In order for a privacy regime to be truly effective, compliance with it must be mandatory and it must be enforceable by individuals. This can only be achieved by the implementation of IPPs in legislation.

- Enshrining IPPs in legislation indicates the government's firm commitment to the information privacy of its citizens. With the continual advancement of information technology such a commitment is a vital issue for all Queenslanders.

- As observed by the DFYCC, legislative privacy principles should ensure that all new legislation is drafted so as to ensure the adverse effects on the privacy of individuals are minimised. This approach should also encourage agencies to review existing legislation they administer to ensure that it does not infringe the legislative privacy principles and make recommendations for any amendments that are necessary and/or desirable to that earlier legislation to avoid conflict with the principles.

A final point raised in submissions was that IPPs contained in administrative guidelines would be more flexible than those contained in legislation and that this was a real concern given the rapid advances in technology. The committee responds to this concern with the observation that the IPPs which the committee supports are broad in nature and therefore should be able to accommodate most concerns arising in the context of information privacy.

However, the committee also realises that the IPPs may fail to address some information privacy concerns in specific areas (particularly as a result of developments in technology), and that necessary legislative amendment of the IPPs may be delayed. The committee's recommendation in section 6.3 that the Queensland Privacy Commissioner/Committee should be able to issue codes of practice (disallowable by Parliament) covering specified information, agencies activities, industries or professions should address these concerns to a large degree.

Moreover, the committee expects that the Queensland Privacy Commissioner/Committee would actively seek to rectify any deficiencies in the IPPs whether brought about by changes in technology or otherwise.[178]

6.2.4 Recommendation

Recommendation 6 - The committee recommends that the IPPs applicable to Queensland government departments and agencies be implemented in legislation, [the Privacy Act (Qld)], and not by cabinet administrative instructions or other administrative means.

6.3 MODIFYING THE APPLICATION OF THE IPPS BY CODES OF PRACTICE

6.3.1 Background

The committee has thus far endorsed the implementation of a core set of IPPs to apply to Queensland government department and agencies. However, it is recognised that these are broad principles and that there may need to be some mechanism whereby these principles can be tailored to more appropriately suit a particular agency or class or type of activity, information, industry etc.

For example, it was noted in section 6.1 of this report that some departments expressed concern that the IPPs contained in the *Privacy Act* (Cth) may need to be amended to suit a state as opposed to the Commonwealth public sector.

Under Part VI of the *Privacy Act* (NZ) the New Zealand Privacy Commissioner has the ability to issue codes of practice:

- modifying the application of any one or more of the IPPs by:
  - prescribing standards that are more or less stringent than the standards that are prescribed by any such principle;
  - exempting any action from any such principle either unconditionally or subject to such conditions as are prescribed in the code;
- applying any one or more of the IPPs (but not all of those principles) without modification;
- prescribing how any one or more of the IPPs are to be applied, or are to be complied with.[179]

Such a code may apply in relation to any specified information, agency, activity or industry, profession, or calling or class (or any class thereof).[180]

---

178 With respect to the Commissioner's 'reporting' function refer to the discussion in chapter 7 concerning the Queensland Privacy Commissioner's functions.

179 s 46(1) and (2).

180 See s 46(3). A code of practice may also provide for any of the matters set out in s 46(4).

The New Zealand Privacy Commissioner can issue a code of practice either on his/her own initiative or upon the application by any person.[181] Sections 47-49 of the Act detail the usual procedure which must be followed before such a code is issued. This involves the Commissioner issuing a public notice of his/her intention to issue a code, calling submissions on the proposed code, advising persons who will be affected by the code as to its proposed terms, notifying the public once the code has been issued and ensuring that once issued, copies of the code are available for inspection by members of the public.

Codes issued under s 46 are disallowable instruments[182] and whilst a code of practice is in force:

- the doing of an act that would otherwise be in breach of an IPP is deemed not to be a breach of that principle if the action is done in compliance with the code; and
- failure to comply with the code is deemed to be a breach of an IPP.[183]

Provision is also made for the Privacy Commissioner to issue 'urgent' codes of practice if following the usual procedures for their issuance would be impracticable. These 'temporary' codes can remain in force for up to one year.[184]

Despite fears that this provision for codes of practice would result in a plethora of codes, the committee understands that to date there have only been five such codes issued, two of which have now expired. The current codes are the Health Information Privacy Code 1994 (Health Code) which relaced an earlier temporary code[185], the Superannuation Schemes Identifier Code 1995 (which modified IPP 12, the 'unique personal identifier' principle, as to the circumstances in which it applied), and the EDS Information Privacy Code which applies to personal information once held by the government computer services entity but now by the private sector.[186] Other areas in which codes are reportedly being prepared include policing, motor vehicle registry, credit reporting and telecommunications.[187]

As already mentioned in chapter 4, the co-regulatory information privacy scheme proposed for the private sector in the federal Attorney-General's discussion paper of September 1996, also proposed the issuing of codes of practice in relation to a privacy regime for the private sector.

Whilst there would appear to be stronger reasons for the need to issue codes of practice in relation to the private sector, arguably there may be some need to modify the IPPs in relation to the public sector. For example, there may be a legitimate need for codes of practice to be developed in relation to areas such as health, and in areas where there is a justifiable need to share information such as the protection of children and the protection of persons with an impaired decision-making capacity.

---

181 s 47.

182 s 50.

183 s 53.

184 s 52.

185 The issue of privacy and health is discussed further in section 10.2 of this report.

186 Refer to the New Zealand Privacy Commissioner's homepage at http://www.knowledge-basket.co.nz/privacy/welcome.htm

187 R Haines, 'The Office and Functions of New Zealand's Privacy Commissioner', *Government Information Quarterly*, vol 13, no 3, 1996, pp 255-274, p 257.

In a 1997 consultation document, Victoria also proposed as part of its data protection regime, to have a code of practice system. Under this system both departmental and industry-focussed data protection codes would be able to be developed in consultation with its state Privacy Commissioner. Thus, these codes would also allow for the tailoring of the IPPs to the particular activities and needs of different government and industry sectors. Victoria also proposed to give these codes statutory backing under its regime.

6.3.2 Arguments raised in public consultation

Whilst few submissions canvassed the direct issue of whether a Queensland Privacy Commissioner/Committee should be able to issues codes of practice modifying the application of IPPs, a number of submissions highlighted problems that could occur if the IPPs in the *Privacy Act* (Cth) were adopted without modification in the case of the provision of certain services.

For example, in a detailed submission the DFYCC stressed that any IPPs introduced into Queensland should not prevent the essential communication and coordination amongst agencies to ensure public safety, particularly in the case of the protection of children. The department stated that in some instances the necessary coordinated approach would breach privacy principles identical to those currently enshrined in the *Privacy Act* (Cth) unless they were amended to incorporate a child protection exception.

The DFYCC further stressed the need for special attention to be given to the impact of the introduction of IPPs to the Queensland government on records relating to people with an impaired decision-making capacity. In particular, the department submitted that the capacity of such persons to provide informed consent to the collection, use and disclosure of personal information must be considered.

In this regard the department referred to the current proposals for implementation of the recommendations of the Queensland Law Reform Commission (QLRC) in relation to assisted and substituted decisions[188] but noted that until these proposals proceed there is no existing statutory mechanism by which consent for the collection, use and disclosure of the records of persons with a decision-making disability can be provided.[189]

The department recommended an interim procedure for authorisation which includes family members or close friends and reflects the recommendations of the QLRC. The department also submitted that if Queensland is to adopt the Commonwealth IPPs then some modifications would be appropriate. For example, the department submitted that IPPs 10 and 11 should be amended so as to permit use and disclosure of personal information where reasonable necessary for the protection of children and people with impaired decision making capacity.

The QCCL also submitted that, in addition to legislative IPPs, there should be a mechanism by which subordinate legislation could be used to rapidly respond to changing developments in technology and privacy protection. The Council further saw a role for a Privacy Committee/Commissioner in advising on, and overseeing, that subordinate legislation.

---

188 Queensland Law Reform Commission, *Assisted and Substituted Decisions*, Report No 49, August 1996.

189 The Powers of Attorney Bill 1997 (Qld) is, at the time of writing, before the Queensland Legislative Assembly.

6.3.3 Analysis and conclusion

The committee believes that a certain degree of flexibility must be built into an IPP regime. In particular, there would appear to be strong arguments for some mechanism which recognises that that modification of the IPPs may be justified in the case of a specific agency or in relation to a class of information or activity that occurs across a number of agencies. This flexibility may be more relevant in the case of privacy principles to apply to the private sector. However, it may also be necessary in the case of IPPs to apply to the public sector.

The DFYCC submitted that specific provision may need to be made for the protection of certain persons in the community (namely children and persons with an impaired decision-making capacity) which requires the sharing of information. In this regard, the committee also notes that the ALRC in its submission to Victoria's DPAC recommended that the IPPs contained in the *Privacy Act* (Cth) were not in an appropriate form to apply to the provision of services such as child care, aged care and disability services.[190] These recommendations flowed from the ALRC's previous reports into these areas.[191]

The ALRC recommended that in these three areas the IPPs needed to be varied in collaboration with the federal Privacy Commissioner and made legally binding in accordance with the current practice in s 13 of the *Privacy Act* (Cth).[192] Section 13 provides that for the purposes of the *Privacy Act*, an act or practice is 'an interference with the privacy of an individual' if the act or practice, amongst other matters, constitutes a breach of specified guidelines in force under other legislation. Thus, it would appear that the ALRC was proposing specific privacy principles in legislation other than the *Privacy Act* but in relation to which the Privacy Commissioner would still have jurisdiction due to s 13.

The committee recognises that particular provision may be required in the case of IPPs relating to children, persons with an impaired decision-making ability and the aged, and that further consideration should be given to the ALRC's previous inquiries in these areas. However, the committee also believes that any appropriate variation to the IPPs may be able to be effected by a mechanism other than by an equivalent to s 13 of the *Privacy Act* (Cth). For example, these areas could be catered for by the Queensland Privacy Commissioner/Committee issuing a code of practice. A further, but less preferable, alternative would be for these areas to be addressed via the 'public interest determination' process discussed in section 6.4 of this report.

Therefore, the committee believes that the Queensland Privacy Commissioner/Committee should have the ability to issue codes of practice specific to a particular agency or in relation to any specified information, activity, profession industry or class (or any class thereof). Part VI of the New Zealand *Privacy Act* would appear to be an appropriate model on which any such provisions are based. In particular, the committee agrees with the following features of that Part:

- the Commissioner's ability to issue codes of practice either on his/her own motion or upon application;

---

190 ALRC, October 1996, op cit, p 6.

191 ALRC Report No 79, *Making Rights Count - Services for people with a disability*, 1996 and ALRC Report No 72, *The coming of age - New aged care legislation for the Commonwealth*, 1995 and ALRC Report No 70, *Child Care for Kids*, 1994.

192 ALRC, October 1996, op cit, p.6.

- the procedures that must be followed in relation to the issuing of codes (including the ability to issue urgent codes where circumstances warrant);
- the fact that the codes of practice are disallowable instruments; and
- the fact that failure to comply with a code is deemed to be a breach of an IPP.

The committee has already flagged that health may be an area in relation to which a code of practice needs to be issued. (The issue of privacy and health is discussed more specifically in chapter 10.)

6.3.4 Recommendation

Recommendation 7 - The committee recommends that the Queensland Privacy Commissioner/Committee be able to modify the application of the IPPs by way of codes of practice to be promulgated as disallowable instruments. The committee further recommends that the provisions relating to codes of practice be modelled on those contained in Part VI of the *Privacy Act 1993* (NZ).

6.4 EXCEPTIONS TO COMPLIANCE WITH THE IPPS

6.4.1 Background

There will obviously be some circumstances in which compliance with a privacy regime should not be required or enforced. Exceptions to compliance will be necessary where the public interest in an agency doing an act or practice in contravention of an IPP substantially outweighs:

- the public interest in adhering to that IPP; or
- the interference with the privacy of an individual which could result from the activity which constitutes the breach.

Obvious situations in which the public interest would warrant an exception to compliance with a privacy principle are where non-compliance is permitted by law, or is necessary for law enforcement or medical emergencies. For example, one would expect that in the case of a patient requiring an urgent blood transfusion a doctor should be permitted to access that person's personal medical records to establish their blood type.

Such 'obvious' exceptions are specifically incorporated in the *Privacy Act* (Cth) IPPs.

With respect to the *use* of personal information, IPP 10 provides that a record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use that information for any other purpose unless, amongst other matters:

- the individual concerned has consented to the use of the information for that other purpose;
- the record-keeper believes on reasonable grounds that use of the information for that

other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

- use of the information for that other purpose is required or authorised by or under law;
- use of the information for that other purpose is reasonable necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
- the purpose for which the information is used is directly related to the purpose for which the information was obtained.

The principle goes on to state that where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Similar exceptions apply in relation to the *disclosure* of personal information to third parties as provided for in IPP 11.

IPPs 10 and 11 of the *Privacy Act* (NZ) also relate to the use and disclosure of personal information and contain comparative exceptions to their Commonwealth *Privacy Act* counterparts.

The federal Privacy Commissioner's recently released *National Principles for the Fair Handling of Personal Information* also contain comparative exceptions. For example, Principle 2.1 provides that an organisation should only *use or disclose* personal information where, amongst other matters:

- the person has consented to the use or disclosure;
- the organisation reasonably believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person's life or health;
- the organisation has reason to suspect that unlawful activity has been engaged in and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to the relevant authorities;
- the use or disclosure is required or specifically authorised by law;
- the use or 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; and
- an intelligence or law enforcement agency asks the organisation to use or disclose the personal information on the basis that the use or disclosure is necessary to safeguard the national security of Australia.

However, the federal Privacy Commissioner does also note that the scope of the exceptions relating to 'law enforcement and revenue protection' and 'national security' are particularly contentious and will have to be reviewed.[193]

The IPPs which deal with *access* by individuals to their own personal information also contain certain exceptions.

IPP 6 of the *Privacy Act* (Cth) provides that an individual is entitled to access to a record of personal information kept by a record-keeper *except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.* In practice, the most relevant 'applicable provisions' are those in the *Freedom of Information Act 1982* (Cth) which sets out a list of exceptions to the right of access.

The right of access to one's own personal information in IPP 6 of the *Privacy Act* (NZ) is also not an absolute right. Part IV of the Act sets out what are 'good reasons' for an agency to refuse to provide an individual with personal information held about them by that agency. These good reasons include security, defence, international relations, trade secrets and prejudicing a supplier's or subject's commercial position.[194] An individual denied access to information under these provisions can complain to the Privacy Commissioner alleging an interference with privacy if an agency exercises its discretion under these provisions in an arbitrary manner.

Similarly, Principle 6.1 of the February 1998 'National Principles' also provides that if requested to do so, an organisation should provide a person with *access* to the personal information it holds about him or her except where, amongst other matters:

- providing access would pose a serious and imminent threat to the life or health of any individual;
- providing access would have an unreasonable impact upon the privacy of other individuals;
- providing access would be unduly onerous for the organisation;
- providing access would be likely to prejudice an investigation of possible unlawful activity;
- providing access would otherwise be unlawful; or
- denying access is specifically authorised by law.

Public interest determinations

In addition to the exceptions contained within the Commonwealth IPPs themselves, Part VI of the *Privacy Act* (Cth) also makes provision for the federal Privacy Commissioner to make a 'public interest determination'. In essence, s 72 of the Act provides that where the Commissioner is satisfied that an act or practice of an agency breaches or may breach an IPP and the public interest in the agency doing the act or practice outweighs to a substantial

193 Federal Privacy Commissioner, February 1998, op cit, p 16.
194 See ss 27-29.

degree the public interest in complying with that IPP, then the Commissioner may make a written determination to that effect. If the agency then does that act or practice whilst that determination is in force, it shall be disregarded for the purposes of the Act.

The procedure regarding the making of such determinations is also outlined in Part VI of the Act. In essence, after an application for a determination is made the Commissioner prepares a draft determination in relation to which a conference of interested parties *may* be held if a party so desires. The Commissioner then makes a decision based on the application and that conference, if held. The Commissioner's final determination is a disallowable instrument.

Examples of areas in relation to which the federal Privacy Commissioner has made public interest determinations include:

- the disclosure of personal information to the Victorian Mental Health Board to assist the Board in assessing whether individuals (with a criminal history) should be continued to be detained in mental institutions;

- the disclosure of police reports for the purposes of pursuing insurance claims or civil litigation; and

- the disclosure of modified electronic white pages to law enforcement agencies for law enforcement purposes.[195]

Similarly, the South Australian Privacy Committee has the ability to exempt a person or body from complying with one or more of the IPPs on such conditions as the committee thinks fit.[196] Examples of matters which in relation to which the committee has granted exemptions include the release of information by the South Australian Police Department to the Accident Research Unit of the University of Adelaide, and the release of information by the State Electoral Commission to the South Australian Cervix Screening Program.[197]

A number of other specific exemptions from the IPPs including a 'public interest' exemption are also contained in Part VI of the *Privacy Act* (NZ).

6.4.2 Arguments raised in public consultation

Some submissions to the committee, whilst supportive of the implementation of IPPs, were also careful to point out the need for those principles to recognise the important balance between an individual's privacy as against a wider public interest.

A number of public sector authorities stressed the need for any privacy regime to allow the government to collect, store, use and disclose information in order to perform functions in the public interest such as law enforcement, protecting public revenue and detecting and ensuring the prosecution of offences relating to evasion and fraud.

As already noted, the Department of Justice recommended a three-staged approach to the implementation of a privacy regime for the public sector. Stage two of this approach includes

---

195 Details of public interest determinations are contained in the *Federal Privacy Handbook*, CCH Publications, Sydney, New South Wales, 1992.

196 See clause 4 of the Proclamation establishing the committee dated 6 July 1989.

197 Exemptions granted by the committee are required to be noted in its annual reports. These particular examples are drawn from the committee's annual report for the year ended 30 June 1994, pp 11-13.

the development of guidelines or principles and accompanying exemptions for the protection of information held by state government departments and agencies. In this regard the Department referred favourably to the public interest determination processes applicable in the Commonwealth and South Australia.

Thus, the department recommended that the Queensland Privacy Commissioner should be able to make a written determination that an act or practice which breaches an IPP may nevertheless be allowed if the public interest in the agency doing that act outweighs the public interest in adhering to the principle.

Specific areas in which exceptions to compliance with a privacy regime were also raised in other submissions. The exceptions noted by the DFYCC have already been canvassed in the previous section. Two other particular exceptions are dealt with below.

Law enforcement

A number of submissions expressed concern about the impact that a privacy regime may have on law enforcement activities. In particular, these concerns are:

- IPPs modelled on IPPs 10 and 11 of the *Privacy Act* (Cth), whilst appropriate in a federal law enforcement sphere, do not reflect the wide 'community policing' functions performed by state police services;

- an interpretation of the 'criminal law' exception in those IPPs would include federal and state criminal law but not include the criminal law of a foreign country, and therefore would restrict the supply of intelligence to foreign jurisdictions even though those jurisdictions may provide information which would assist in enforcing Australian criminal laws; and

- the different interpretations which may be given to the term 'enforcement' as it appears in those IPPs.

Recommendations made to the committee as to how to overcome these concerns included:

- the exemption of law and order matters from any privacy regime which included IPPs;

- in order to bring the principles into line with the 'community policing' functions and responsibilities of state policing operations, amending IPPs 10 and 11 to include the words, 'a policing function' after the words 'criminal law' in sub clause 1(d) and (2) of IPP 10 and in sub clause 1(e) and 2 of IPP 11;

- amending any IPPs based on the *Privacy Act* (Cth) to clearly reflect that 'enforcement of the criminal law' includes:

  - the investigation of a *suspected* breach of the criminal law; and

  - the gathering of information for legitimate intelligence purposes, even though a specified identified incident of a suspected breach of the criminal law is not being investigated.

The CJC also suggested that a privacy regime which recognises the role of use and dissemination of information for legitimate law enforcement purposes, should place on the law

enforcement agency seeking the information the onus of showing that particular personal information is required for a law enforcement purpose. In this regard the CJC favoured a certification process whereby a designated senior officer of the law enforcement agency seeking the information could certify that the information was reasonable necessary for law enforcement purposes (or an investigation of suspected official misconduct in the case of the CJC) and the information-holder could accept that certification.

Further, the CJC advised the committee that a privacy regime should not allow unlawful conduct to be easily hidden from detection and examination. The CJC stressed that under current legislation a 'whistleblower' is only provided protection in respect of 'public interest disclosures' which are defined relatively narrowly. Therefore, whilst there is potentially a public benefit in a person blowing the whistle, the whistleblower is in a difficult situation if he/she is acting primarily on his/her own personal knowledge (as is usually the case). The CJC concluded that any privacy regime must be drafted to take into account situations which justify a person whistleblowing and ensure that protection offered to them is not diminished.

The University of Queensland also expressed concern should Queensland adopt a principle similar to IPP 11 of the *Privacy Act* (Cth) regarding the exception to non-disclosure which applies in relation to law enforcement. Whilst supporting law enforcement agencies in their endeavours to ensure that its campuses are free from criminal activity the university also stated that it:

> *… would be most concerned that the traditional independence from government of this and other Universities will be undermined if this exception to the limitations on disclosure were to be invoked by law enforcement agencies pursuing more generalised intelligence gathering functions. It is the University's submission that any legislative or administrative scheme which is put in place should recognise that, if this exception to non-disclosure is invoked in accordance with Information Privacy Principle 11, that agencies be provided with sufficient information to determine that the request is based on legitimate law enforcement grounds.*[198]

The provision of information by, and to, the Electoral Commission of Queensland

The Electoral Commission of Queensland (ECQ) submitted that it is in two main areas that tensions may arise between the ECQ's performance of its powers and functions under the *Electoral Act 1992* and any privacy legislation. These areas are:

- the ECQ's exercise of its discretion to allow data on the *entire* (that is, both public and non-public information kept on the roll) electoral roll to be supplied to certain state departments and agencies in the overall public interest of Queenslanders (for example, electoral roll data is used for certain health programs such as the treatment and prevention of tuberculosis); and

- the proposal to seek relevant data from state agencies which could be "data-matched" by the Australian Electoral Commission for Continuous Roll Updating (CRU) purposes so that the joint electoral roll in Queensland is as accurate and current as possible.

Thus, the ECQ submitted that:

[198] University of Queensland letter dated 25 July 1997, p 1.

> *…it is vital that any State privacy legislation not impede the dissemination of information held on the entire roll to approved State Government agencies (provided always that the public interest in distributing the information outweighs any privacy considerations), nor the CRU process, which aims to make Australia's electoral roll more accurate more of the time.*[199]

With respect to the CRU process, the ECQ advised the committee that the optimum outcome from its viewpoint would be that the supply of information for data-matching CRU processes be exempt from any state privacy legislation or, more significantly, provide the ECQ with legislative power to obtain essential information for roll keeping purposes similar to that contained in s 92(1) of the *Commonwealth Electoral Act 1918*.

The need for certain persons and bodies to have access and use of public-record information

A number of private and public sector organisations and bodies also submitted to the committee that access to a range of public-record information such as that from the courts, vehicle registers, licensing authorities and various title and security interest registers is necessary and ultimately in the public interest.

For example, the Australian Bankers' Association (ABA) stressed that banks and other financial institutions rely heavily on the ability to interrogate public databases such as registries relating to land titles, bills of sale, powers of attorney, and other many and varied bodies holding registration or licensing details covering other businesses, professions and other activities.

In the words of the ABA:

> *The ability to verify the identity of the registered proprietor of land, to ascertain the nature and extent of registered interests affecting the property of a customer and to verify other information (for example, such as a business name) are basic information needs in the course of carrying on business.*
>
> *Therefore, it is imperative that general freedom of access to such information is maintained and that no fetters or impediments are placed on access or on the uses for which that information may legitimately be put. For example, a creditor seeking the whereabouts of an errant debtor will frequently access public database information to assist in this pursuit.*[200]

The Australian Finance Conference made similar comments:

> *Members have a bona fide commercial need for this data usually to protect or preserve their security interest in items owned or financed by them to vouchsafe the representations made to them by those seeking finance. In these circumstances there is a natural balancing of privacy rights with commercial and other community needs for the better functioning of markets and optimal pricing of goods and services.*[201]

The Credit Reference Association of Australia Ltd also advised the committee that any limitation on access to such information would have an immediate impact on the cost of credit in Queensland.

---

199 Electoral Commission Queensland, submission dated July 1997, p 18.

200 Australian Bankers' Association, submission dated 30 July 1997, p 2.

201 Australian Finance Conference, submission dated 1 August 1997, p 4.

Similarly, the Insurance Council of Australia submitted that any proposed privacy regime needed to provide the insurance industry with clear powers to obtain information from the public sector when authorised and appropriate to do so. The Council warned that if insurers did not have the ability to obtain or verify information, *consumers could be disadvantaged by having insurers decline their risks or having to pay a higher level of premium than their personal circumstances would otherwise merit.*[202]

Some public sector organisations were also concerned that legislation permitting them to undertake activities such as conducting background checks into potential employees in certain sensitive industries and keeping registers of licensees was not affected by privacy legislation.

For example, the Building Services Authority (BSA) is required by statute to keep a register of licensees. This register also contains information pertaining to the licensee including details of any disciplinary action taken and any directions to rectify defective work. In this regard the BSA submitted:

> *Such detail is an essential component of the BSA's consumer advice objective allowing consumers to obtain information which may be crucial in the choice of Builder/Trade Contractor and which may otherwise be unavailable. The BSA would seek to ensure that the statutory right to maintain the register and provide reports indicating contractor performance is not affected by the introduction of legislation governing privacy in Queensland.*[203]

6.4.3 Analysis and comment

The committee has stated from the outset of this report that it recognises that situations will arise in which the public interest in an agency doing an act or engaging in a practice in breach of an IPP will outweigh the public interest in adhering to the principle. Recognition of the need to cater for this 'balance' in a privacy regime is evident from the 'public interest' exceptions made in the privacy regimes of the various jurisdictions as noted above.

The committee has already recommended one procedure which could result in exceptions to the IPPs; namely, the 'code of practice' procedure discussed in section 6.3 whereby the IPPs can be modified to suit particular agencies, industries, activities, information etc. However, the committee agrees with the approach taken in the Commonwealth and New Zealand legislation that there should be other processes pursuant to which exceptions can be made. In particular, the committee believes that certain exceptions should be contained in the IPPs themselves and that provision should be made for other exceptions to result from a 'public interest' determination process.

<u>The exceptions to be contained in the IPPs</u>

As already noted, the exceptions which appear in the Commonwealth IPPs themselves generally relate to access, use and disclosure of personal information in cases of consent, serious and imminent threat to life or health, authorisation by law, and law enforcement. Justification for this approach would appear to be that in these circumstances the public benefit clearly lies in favour of using or disclosing the information and time will often be of the essence.

---

202 Insurance Council of Australia Limited, submission dated July 1997, p 7.

203 Building Services Authority, submission dated 16 July 1997, p 1.

The committee believes that many of the problems foreseen with an information privacy regime for Queensland will be dealt with by adopting IPPs with the same exceptions. This is particularly so in the case of the 'required or authorised by law' exception. The introduction of a privacy regime will apply over the top of existing law and therefore will not operate to prevent any practices that are expressly authorised elsewhere. The only cases in which problems will arise is where practices lack any authority and breach the principles. Therefore, this should allay many of the concerns expressed in submissions regarding the keeping of, and access to, registers as permitted by law.

In addition, it is also important to bear in mind that the exceptions to these non-disclosure principles do not confer on record-keepers a general 'authority' to disclose information. In other words, a record-keeper is not obliged to disclose information simply because an exception allows disclosure - unless, of course, it is required by law.

On this basis, the committee endorses the adoption of the exceptions contained in the Commonwealth IPPs in the Privacy Act (Qld).[204] However, the committee does have some minor concerns with the exceptions as they currently appear in the Commonwealth IPPs.

The committee is concerned that in some circumstances the 'protection of the public revenue' exception could, without proper limitation, be too wide.[205] For example, it could be used as authority to conduct large-scale data matching which at the end of the day nets few 'fraud' cases yet in the process infringes the privacy rights of many. Therefore, the committee believes that in such cases an additional 'balance' mechanism should be inserted.

The committee favours as this additional balance mechanism, a certification process similar to that recommended by the CJC in relation to law enforcement bodies. It is proposed that this would entail a process whereby a designated senior officer of the public revenue collection body seeking information must certify that that particular personal information is required for public revenue protection purposes. Therefore, an officer in the agency takes responsibility for the decision to seek the information and the person in the agency providing the information has a certification document on which they can rely if the disclosure of the information is called into question.

The submissions with respect to law enforcement also related to the exceptions contained within the IPPs themselves. Two main recommendations emanated from submissions in this regard. Firstly, it was proposed that 'law and order matters' should be exempted from any IPP regime. Alternatively, it was proposed that any law enforcement exceptions to be contained in the IPPs should:

- reflect the wider community policing functions;
- be interpreted to include the law of a foreign country;
- not restrict the gathering and supply of intelligence (including the supply of intelligence to foreign jurisdictions); and
- include investigation of a *suspected* breach of the criminal law.

---

[204] In particular this refers to IPP 6, 10 and 11.

[205] The House of Representatives Standing Committee on Legal and Constitutional Affairs also expressed similar concerns in its *In Confidence* report, op cit, pp 65-68. Recommendation 21 of that report was that the *Privacy Act 1988* (Cth) be amended to clarify that term.

It was further submitted that a certification process be introduced whereby a designated senior officer of the law enforcement agency seeking particular personal information bears the onus of showing that that information is required for law enforcement purposes.

The committee does not believe that there should be a blanket exemption of law and order matters from a privacy regime. Such an exception would be too wide and could potentially undermine the intent of the regime. In fact, that committee notes that there have been recommendations to narrow this exception as it appears in the Commonwealth *Privacy Act* due to the liberal interpretation given to words 'reasonably necessary'.[206]

However, the committee also recognises the arguments raised in submissions in the law enforcement context and believes that:

- the issues noted above should be considered in the drafting of any law enforcement exceptions and, where appropriate, further consultation with law enforcement agencies should take place; and

- for the reasons outlined above in relation to the 'public revenue protection' exception, a certification procedure such as that recommended by the CJC should be adopted. (The adoption of this certification process would also seem to address the concerns expressed by the University of Queensland.)

However, the committee does stress in relation to the certification procedure for both law enforcement and revenue protection purposes that certification should be done on a case by case basis. The committee cautions that this process should not be used for bulk disclosures of classes of information.[207]

The committee further endorses the concept of the requirement currently contained in IPPs 10.2 and 11.2 that where personal information is used or disclosed for the enforcement of the criminal law or the protection of public revenue, then the record-keeper should be required to include in the record containing that information a note of that use or disclosure.

The CJC also submitted that any privacy regime must be drafted to take into account situations which justify a person whistleblowing and ensure that protection offered to them is not diminished. In this regard the committee observes that IPPs deal with the behaviour of 'agencies' and not that of individuals acting in their capacity as such. Therefore, the committee believes that whilst any privacy regime should have regard to the protection of 'whistleblowers' and ensure that protection offered to them is not diminished, whistleblower protection is more to do with providing exceptions or defences to breaches of confidentiality than with a privacy regime such as it is proposing.

A 'public interest' determination process

With respect to the other specific exceptions raised in public consultation, the committee believes that many of these can be addressed by the Queensland Privacy Commissioner/Committee having the ability to make 'public interest determinations' in the same way that the federal Privacy Commissioner may under Part VI of the *Privacy Act* (Cth).

206 Ibid, pp 65-67.

207 See the concerns of the federal Privacy Commissioner regarding such 'bulk' disclosures in the *In Confidence* report. Ibid, p 66.

For example, a public interest determination could be made in relation to the Electoral Commission of Queensland (ECQ) providing data from the *entire* electoral roll (that is, including non-publicly available information kept on the roll) to be supplied to certain state departments and agencies in respect of specified health programs.

In relation to the other concern raised by the ECQ, the committee notes that the issue of the Australian Electoral Commission (AEC) using Continual Roll Updating is raised by the federal Privacy Commissioner in her latest annual report.[208] There the Commissioner states that whilst she recognises the need for integrity and accuracy of the electoral roll and the sense in the use of more efficient means to this end, her main concern is that the update should be conducted in line with acceptable privacy practices. The Commissioner reports that she has discussed her concerns regarding this proposal with the Australian Joint Roll Council and that the issue is still the subject of ongoing discussions with the AEC and Joint Roll Council.

The committee therefore believes that any exceptions to be made in this regard should be made in consultation with both the ECQ and the federal Privacy Commissioner.[209]

Access to public registers

The committee recognises the legitimate needs of some businesses and individuals to have access to personal information held on public registers. In many cases access to public registers will not be prevented by the IPPs if Queensland adopts the Commonwealth definition of 'record' as it does not include a 'generally available publication'. In other cases, this access will be permitted by the exception to disclosure under IPP 11, that is, 'the disclosure is required or authorised by or under law'. [For example, the searching of land title records is authorised under s 35(1) of the *Land Title Act 1994* (Qld).]

However, computer programs which now allow the searching, matching and analysis of public register information means that this data may be used for purposes other than those originally intended. In particular, this information can be used for marketing purposes. In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs recommended that the federal Privacy Commissioner coordinate a review of the reasons for allowing access to public registers including whether any limits need to be imposed on the purposes for which such information can be used.[210]

In this context it is also relevant to note that Part VII of the *Privacy Act* (NZ) contains four public register privacy principles (PRPPs). These principles are as follows.

PRPP 1 - Personal information shall be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organised.

PRPP 2 - Personal information obtained from a public register shall not be re-sorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.

---

208 Federal Privacy Commissioner, *Ninth Annual Report*, op cit, pp 21-22.

209 For further discussion on the provision of information from the Commonwealth electoral roll see the *In Confidence* report, op cit, pp 149-152.

210 Ibid, pp 148-149.

PRPP 3 - Personal information in a public register shall not be made available by means of electronic transmission, unless the purpose of the transmission is to make the information available to a member of the public who wishes to search the register.

PRPP 4 - Personal information shall be made available from a public register for no charge or for no more than a reasonable charge.[211]

Agencies responsible for administering a public register are to comply, as far as is reasonably practicable, with the IPPs and the public register privacy principles.[212] The New Zealand Privacy Commissioner may, either on complaint or on his/her own initiative, inquire into any public register provision if it appears to the Commissioner that the provision is inconsistent with any of the IPPs or any of the PRPPs.[213] However, the public register privacy principles do not confer on any person any legal right that is enforceable in a court of law.[214]

The Privacy Commissioner may also issue a code of practice in relation to any public register.[215]

The committee has not undertaken a detailed analysis of the need and/or desirability of public register principles, nor has it carried out specific consultation in this regard. However, the committee believes that this is a task that the Queensland Privacy Commissioner/Committee should conduct soon after the establishment of that office.

6.4.4 Recommendation

Recommendation 8 - The committee has already recommended that the Privacy Act (Qld) contain a set of IPPs substantially modelled on those contained in s 14 of the *Privacy Act 1988* (Cth). The committee confirms that it also recommends the inclusion of the exceptions contained in the Commonwealth IPPs in those IPPs, subject to the following comments.

Firstly, in relation to the 'public revenue protection' exceptions, the committee recommends that an additional balance mechanism should be introduced. This mechanism should be a certification process whereby a designated senior officer of the public revenue collection body seeking personal information from a department or agency must certify to the department or agency that that *particular* information is required for public revenue protection purposes.

Secondly, in relation to the law enforcement exceptions, the committee recommends that:

- **the issues raised in the committee's consultation process and noted in the discussion above should be considered in the drafting of any law enforcement exceptions and, where appropriate, further consultation with law enforcement agencies should take place;**

---

211 Although the committee does note that PRPP 4 does not appear to concern privacy as such.

212 s 60(1).

213 s 61.

214 s 62.

215 The provisions relating to public register codes of practice and their effect are set out in ss 63-64 of the *Privacy Act* (NZ).

- **there should be a certification process introduced whereby a designated senior officer of a law enforcement agency seeking personal information from a department or agency must certify to the department or agency that that *particular* information is required for law enforcement purposes; and**

- **any privacy regime should have regard to the protection of 'whistleblowers' and ensure that protection offered to them is not diminished.**

In addition, the committee recommends that:

- **the Privacy Act (Qld) contain a Part modelled on Part VI of the *Privacy Act 1988* (Cth) pursuant to which the Queensland Privacy Commissioner/Committee will have the ability to make public interest determinations; and**

- **the Queensland Privacy Commissioner/Committee conduct further inquiry and consultation with respect to the need and/or desirability of public register privacy principles such as those contained in Part VII of the *Privacy Act 1993* (NZ).**

6.5 THE APPLICATION OF IPPS TO INFORMATION ALREADY HELD

6.5.1 Background

An important issue which must be determined in relation to the implementation of a privacy regime is its application to information already held.[216]

Section 15 of the *Privacy Act* (Cth) provides that certain of the IPPs apply in relation to information collected after the commencement of the Act, whilst others apply in relation to information contained in a record held by an agency regardless of whether the information was collected before or after the commencement of the Act.[217]

Those IPPs which only apply in relation to information collected *after* the commencement of the Act concern:

- the manner of collection of personal information (IPP 1);

- the purpose for which personal information is collected (IPP 2);

- the accuracy and relevance of information collected (IPP 3);

- limits on use of personal information (IPP 10); and

- limits on disclosure of personal information (IPP 11).

Those IPPs which apply in relation to information contained in a record held by an agency regardless of whether the information was collected *before or after* the commencement of the Act concern:

---

[216] Whilst this is often referred to as 'retrospective operation' of the IPPs the use of the term 'retrospective' in this regard should be distinguished from a situation in which legislation truly applies retrospectively, that is, where it applies to conduct which occurred prior to its commencement.

[217] s 15.

- the storage and security of personal information (IPP 4);
- the maintenance of records kept by a record-keeper (IPP 5);
- access to records containing personal information (IPP 6);
- alteration of records containing personal information (IPP 7);
- the requirement for record-keepers to check the accuracy etc of personal information before use (IPP 8); and
- the requirement that personal information is only to be used for relevant purposes (IPP 9).

In his September 1996 discussion paper *Privacy Protection in the private sector*, the federal Attorney-General proposed that the application of the IPPs be altered from the current position. In particular, it was proposed that IPPs 10 and 11 governing the use and disclosure of personal information would apply to information collected both before and after the commencement of the regime.[218]

The issue of 'retrospective' operation of a privacy regime is also canvassed in the federal Privacy Commissioner's consultation paper of August 1997 *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector*. Although this paper relates to privacy in the private sector, similar considerations should apply in respect of the operation of a privacy regime applicable to the public sector.

In particular, the federal Privacy Commissioner notes concerns expressed by some that it would be impracticable to try and apply IPPs to information already held by organisations. The federal Privacy Commissioner concludes that a common sense approach will have to be taken in relation to this question and that the guiding idea should be that the principles apply as far as possible to all personal information except where that is clearly impractical or unfair to the organisation.[219]

Further, with reference to the modified IPPs proposed in that paper for the private sector the federal Privacy Commissioner notes:

> *The collection, limitation and notification principles clearly cannot operate retrospectively. The use limitation principle should apply as far as it can to existing information although this may not always be feasible, for example, where an organisation collected information in the expectation of using it for a secondary purpose but did not need at that time to seek people's consent. The security and openness principles could probably apply to all personal information. The destruction and quality principles could apply to all personal information but organisations obviously cannot be expected immediately to review all the personal information they hold. The access and correction principles could apply to all factual information but there would need to be some exceptions to cover opinion or evaluative material information collected on the assumption that it would not be accessible to the individual.*[220]

---

218 Federal Attorney-General, op cit, p 12.

219 Federal Privacy Commissioner, op cit, p 36, para 175.

220 Federal Privacy Commissioner, op cit, pp 36-37, para 176.

The above paragraph indicates some modification to the approach taken in s 15. In particular, the federal Privacy Commissioner notes that the proposed use limitation (which broadly incorporates the current use and disclosure principles) should apply as far as it can to existing information although recognising that this may not be feasible in some situations. This differs from s 15 which states that the use and disclosure IPPs only apply to information collected *after* the commencement of the Act.

The second modification which the Commissioner suggests is in relation to the access and correction principles. In this regard she states that they could apply to all factual information but there would need to be some exceptions to cover opinion or evaluative material information collected on the assumption that it would not be accessible to the individual. In this regard s 15 currently provides that the IPPs concerning access and alteration to records containing personal information apply in relation to information whether collected before or after the commencement of the Act. There is no provision for opinion or evaluative material information.

This proposed modification would appear to be more in line with private sector considerations, however, there may be some instances in which access to some material held by the public sector should be selective. In particular, there is a strong argument that 'retrospective' access to certain health records should be limited.

The issue of retrospective operation of a privacy scheme in relation to health records (held by both the public and private sectors) was considered by the ACT in its recent position paper *Health Records: Privacy and Access*.[221] It was noted in that paper that many health service providers argue strongly against any legislation giving health consumers access to their health records retrospectively on the basis that some of those may record their own thoughts, opinions, and ideas. They further argue that if they had known at the time of preparation of the record that in the future it would be able to be accessed by the person concerned then they may have prepared the record in a different, perhaps more 'circumspect' manner.[222]

These reservations do not however apply to 'matters of fact' which the paper notes would seem to include information with respect to a patient's history, findings on physical examination, results of investigations, diagnoses and any proposed plan of management or action carried out under such a plan.[223]

Thus, the paper concludes that the then proposed ACT legislation with respect to health records held by both the public and private sectors should only apply to health services and records or entries made on an existing record where these occurred after the date of commencement of the new law. However, in the cases where matters of fact are concerned, a person will have a right of access to these whenever the records were prepared. It is further specifically noted that this differs from the current situation under s 15 of the *Privacy Act* (Cth) where the access IPP (IPP 6) is fully retrospective.[224]

---

221 ACT Government, *Health Records: Privacy and Access - An ACT Government Position Paper*, ACT Government Printer, May 1997.

222 Ibid.

223 Ibid.

224 Ibid.

This position is now reflected in s 10 (1) of the *Health Records (Privacy and Access) Act 1997* (ACT) which was passed following the release of this position paper.[225]

6.5.2 Arguments raised in public consultation

The issue of the application of a privacy regime to information already held was not generally canvassed in submissions. However, with respect to the 'retrospective' operation of an access principle in the case of health records, similar concerns to those canvassed in the ACT position paper were raised at the Townsville public hearing by Dr Tony Landgren.

Dr Landgren reiterated that many health records were made by practitioners in times when it was never envisaged that there would be a release of that information, and that often these records contain information in relation to the service provider's thought processes or personal views. Therefore, he suggested that for any scheme to be workable it probably has to apply prospectively in a general sense and, selectively, retrospectively.

6.5.3 Analysis and conclusion

The starting point for considering the 'retrospective' operation of Queensland's proposed privacy regime is logically s 15 of the *Privacy Act* (Cth) given that the committee has recommended that Queensland's IPPs be modelled on those contained in that Act.

Adopting the approach in s 15 would mean that certain IPPs should operate to information collected both *before and after* the commencement of the privacy legislation. These IPPs would be those relating to:

- storage and security of personal information (IPP 4);
- the maintenance of records kept by a record-keeper (IPP 5);
- access to records containing personal information (IPP 6);
- alteration of records containing personal information (IPP 7);
- record-keeper to check accuracy etc of personal information before use (IPP 8); and
- personal information only to be used for relevant purposes (IPP 9).

However, there would also appear to be scope for IPPs 10 and 11 governing the use and disclosure of personal information to also apply to information collected both before and after the commencement of the regime. The federal Attorney-General proposed such an approach in his 1996 Discussion Paper. The federal Privacy Commissioner in her August 1997 consultation paper also suggests that there should be some scope for the use and disclosure principles to also apply to information collected *before* the commencement of any legislation.

The committee agrees that to be effective, a privacy regime should in general apply to restrict the use and disclosure of personal information irrespective of when that information was collected. However, the committee does also agree with the federal Privacy Commissioner that in some cases this approach may not be feasible. As the federal Privacy Commissioner

[225] This issue is raised again in section 10.2 of this report which concerns privacy in the area of health.

points out, it would not be feasible, for example, where an organisation collected information in the expectation of using if for a secondary purpose but did not need at that time to seek people's consent.

There is also a clear argument for special provision to be made in the case of access and correction to certain evaluative material information. One area in particular in which there would appear to be a need for such selective 'retrospective' access in Queensland's public sector is in relation to certain health records. Currently no such special provision exists in the *Privacy Act* (Cth).

In this regard the committee agrees with the approach taken in the ACT position paper; namely, that access and correction principles only apply to health services and records or entries made on an existing record where these occurred after the date of commencement of the new law. However, in the cases where matters of fact are concerned, a person will have a right of access to these whenever the records were prepared.

Clearly principles in relation to certain matters can only apply to information collected after the commencement of the Act. These principles would be those relating to the:

- manner of collection of personal information (IPP 1);
- purpose for which personal information is collected (IPP 2); and
- accuracy and relevance of information collected (IPP 3).

6.5.4 Recommendation

Recommendation 9 - On the basis that the IPPs in the Privacy Act (Qld) are substantially modelled on those contained in s 14 of the *Privacy Act 1988* (Cth), the committee recommends the following:[226]

1. Those IPPs relating to:

- **manner of collection of personal information (IPP 1);**
- **purpose for which personal information is collected (IPP 2); and**
- **accuracy and relevance of information collected (IPP 3);**

apply to personal information collected *after* the commencement of the Privacy Act (Qld).

2. Those IPPs relating to:

- **the storage and security of personal information (IPP 4);**
- **the maintenance of records kept by a record-keeper (IPP 5);**
- **access to records containing personal information (IPP 6);**[227]

[226] References to the IPPs in this recommendation refer to the IPPs currently contained in the *Privacy Act* (Cth).

- **alteration of records containing personal information (IPP 7);**
- **the requirement for record-keepers to check the accuracy etc of personal information before use (IPP 8); and**
- **the requirement that personal information is only to be used for relevant purposes (IPP 9);**

apply to personal information collected both *before and after* the commencement of the Privacy Act (Qld).

3. **Provision be made for the IPPs regarding the use and disclosure of personal information (IPPs 10 and 11) to apply, as far as is reasonably practicable, to information collected both *before and after* the commencement of the Privacy Act (Qld).**

4. **Special provision be made in the case of the access principle (IPP 6) as it applies to certain health records, namely, that that principle will only apply to health services and records or entries made on an existing record where these occurred after the date of commencement of the Privacy Act (Qld). However, in cases where matters of fact are concerned, a person should have a right of access to these records whenever they were prepared.**

6.6 PRIVACY, FREEDOM OF INFORMATION AND ARCHIVES LEGISLATION

6.6.1 Introduction

Should privacy legislation applicable to Queensland's public sector be introduced, then consideration must be given to its interrelationship with other legislation which also relates to access to information held by the government. In Queensland this other legislation is the *Freedom of Information Act 1992* (Qld) and the *Libraries and Archives Act 1988* (Qld).

6.6.2 Privacy and FOI legislation

6.6.2.1 Background

The object of the *Freedom of Information Act* (the FOI Act) is to enhance the accountability of government by providing the community with, a general statutory right to have access to information held by government. This right is, however, limited by certain exceptions relating to protecting the public interest and persons' personal affairs. The FOI Act also enables members of the community to access information held about them so they can ensure that documents held by the government concerning their personal affairs are accurate, complete, up-to-date and not misleading.

Therefore, the interrelationship of the FOI Act with the committee's proposed privacy legislation (which also regulates the access, correction, use and disclosure of information held by the government) must be carefully considered. This raises two issues in particular.

[227] IPP 6 is subject to 4 below.

Consistency in terminology -'personal affairs information' or 'personal information'

The access to information under FOI legislation by one person has the potential to infringe another person's privacy if that information is 'personal' to that other person. The FOI Act recognises that in some cases the privacy of individuals should come before the public interest in disclosure. Therefore, s 44 provides that an agency can exempt from disclosure to third parties certain matter relating to 'information concerning the personal affairs of a person' ('personal affairs information').

Whilst 'personal affairs information' is not defined in the FOI Act, it is generally recognised[228] as not being as broad in scope as the term 'personal information' used in the Commonwealth *Privacy Act*. The term 'personal affairs information' is also used in the amendment of information provisions in the FOI Act (which are discussed later in this section).

Therefore, the adoption of IPPs in the Privacy Act (Qld) requires some careful consideration as to the need for consistency in terminology used in that Act and that used in the FOI Act; that is, either 'personal affairs information' or 'personal information'.

The term 'personal affairs information' was used initially in the Commonwealth *FOI Act* but was replaced in 1991 with the term 'personal information' so that it is now consistent with the Commonwealth *Privacy Act*. In the recent joint report by the Administrative Review Council (ARC) and the Australian Law Reform Commission (ALRC) *Open Government: A Review of Federal Freedom of Information Act 1982*[229] it was noted that the reasons for this change appear to have included:

- to ensure that work related information, for example, work performance information which did not constitute 'personal affairs' would be covered by the amendment provisions of Part V of the *FOI Act* (Cth); and
- to make the Commonwealth FOI and privacy legislation consistent in this respect.[230]

Although, the joint review also noted:

> *It* [the term 'personal information'] *encompasses more information than did the pre-1991 term 'personal affairs' and has been interpreted widely. In the FOI context this can be problematic because it raises the prospect of a great deal of information being exempt under s 41* [the Commonwealth FOI exemption from access provision]. *It is therefore important that s 41 achieves an appropriate balance between protecting personal privacy and providing access to government-held information*.[231]

In *Re Stewart and Department of Transport*[232] and later in *Re Pope and Queensland Health*[233] the Queensland Information Commissioner discussed in some detail the meaning of the term 'personal affairs of a person' as it appears in the FOI Act. In *Re Pope* the Commissioner stated in referring to his earlier decision:

---

228 See the interpretation given to 'personal affairs information' by the Queensland Information Commissioner below.

229 ALRC Report No. 77, ARC Report No. 40, Australian Government Printing Service, Canberra, 1995.

230 Ibid, p 126, para 10.3 and footnote 5.

231 Ibid, p 126, para 10.3.

232 (1993) 1 QAR 227.

233 (1994) 1 QAR 616.

> *In particular, I there said that information concerns the 'personal affairs of a person' if it relates to the private aspects of a persons' life; and that while there may be a substantial grey area in the ambit of the phrase 'personal affairs', that phrase has a well accepted core meaning which includes affairs relating to-*
>
> - *family and marital relationships;*
> - *health or ill-health;*
> - *relationships with and emotional ties with other people; and*
> - *domestic responsibilities or financial obligations*.
>
> *Whether or not matter contained in a document comprises information concerning an individual's personal affairs is essentially a question of fact, based on a proper characterisation of the matter in question*.[234]

If the term 'personal affairs information' is used in the Privacy Act (Qld) then it would be consistent with the use of that term in s 44 (the exemption from access provision) of the Queensland FOI Act.

However, adopting that approach raises issues as to (a) whether there is a need for such consistency and (b) whether the use of that term would render the ambit of the privacy regime too narrow. From the discussion in *Re Pope* it would seem that the phrase 'personal affairs' of a person would not include:

- acts, matters or things done by a person in a representative capacity on behalf of another person, body or organisation (because there is no relevance between the information contained in the document and any matter personal to the applicant); and
- information which merely concerns the performance by a government employee of his or her employment duties, that is, their 'vocational competence'.[235]

Thus, the question arises as to whether information such as the above should be covered by a privacy regime.

Depending on the outcome of this issue there may also have to be other consequential amendments to the *FOI Act* (Qld) as a result of the introduction of privacy legislation. In its joint review the ALRC and ARC made several recommendations designed to ensure that disclosures of personal information under the *FOI Act* (Cth) are more in line with exceptions under IPP 11 (the disclosure IPP). These included:

- redrafting s 41 [the Commonwealth FOI exemption provision] to provide that a document is exempt if, amongst other matters, its disclosure would constitute a breach of IPP 11 of the Commonwealth *Privacy Act*[236]; and
- amending the Commonwealth *Privacy Act* to provide that the release of personal information under the FOI Act is deemed to be disclosure that was 'required or

234 (1994) 1 QAR 616 at p 658.
235 (1994) 1 QAR 616 at pp 659-660.
236 ALRC/ARC, op cit, p 128, rec 59.

authorised by law' for the purposes of IPP 11.1(d), provided the consultation requirements in the FOI Act are complied with.[237]

Which legislation should contain access and amendment provisions?

The second area in which consideration must be given to the interrelationship between FOI and privacy legislation, is with respect to the location of provisions relating to access to, and amendment of, an individual's own information. This is because, as noted above, potentially both pieces of legislation will grant persons with access and correction rights.[238]

Section 53 of the FOI Act provides that a person who has had access to a document from an agency or Minister containing information relating to:

- the person's personal affairs; or
- the personal affairs of a deceased person to whom the person is next of kin;

is entitled to apply to the agency or Minister for correction or amendment of any part of the information if it is inaccurate, incomplete, out-of-date or misleading.

IPPs 6 and 7 of the *Privacy Act* (Cth), which the committee has recommended that Queensland adopt, also provide individuals with a right of access to, and amendment of, records containing their own 'personal information'.

Again definitional issues will arise if the FOI Act is to apply to 'personal affairs information' and the Privacy Act (Qld) is to apply to 'personal information'. However, even if consistent terminology is used, there is still an issue as to whether both or only one Act should provide for access to, and amendment of, 'personal information'. Further, if both Acts are to contain these rights then consideration must be given to managing the 'overlap'.

The committee understands that, initially, access and correction rights to personal information were included in the Commonwealth FOI Act pending the introduction of comprehensive privacy legislation. However, despite the subsequent enactment of the Commonwealth *Privacy Act* which contained the access and correction rights set out in IPPs 6 and 7, the access and correction provisions remained in the FOI legislation. Thus, it has developed that access to, and correction of, personal information is handled under the FOI legislation as it provides more detailed mechanisms in this regard.[239]

However, some have argued that access to, and amendment of, one's own personal information should be regulated by the *Privacy Act* alone (and hence the relevant provisions removed from the FOI legislation).[240]

The federal Privacy Commissioner has also stated that access and amendment rights should be administered solely by the Privacy Commissioner. This argument is based on a number of

---

237 Ibid, p 137, rec 65. Whilst the review did recognise that it would unlikely that an agency would be found by the Privacy Commissioner to have breached IPP11 in respect of information disclosed pursuant to the Act, it stated that in the interests of certainty this issue should be clarified.

238 Part 4 of the FOI Act relates to amendment of information.

239 ALRC/ARC, op cit, p 55, para 5.15.

240 Ibid, p 55, para 5.17.

grounds including that the right to access and amend personal information is essentially a privacy right and therefore separate and distinct from the objectives of FOI legislation.[241]

The relationship between the Commonwealth's FOI and privacy legislation was considered by the joint ALRC/ARC review. In particular, the review considered how the overlap between access and amendment rights in the Commonwealth privacy and FOI legislation should be further reconciled.[242]

The joint review concluded that access and correction provisions should not be contained in the *Privacy Act* alone. Its reasoning in this regard included that:

- 'mixed requests' (i.e. requests covering the applicant's personal information and other information) would have to be split and dealt with under two Acts or else classified by agencies to determine under which Acts the whole request should be dealt with and this would be unnecessarily complicated and confusing;

- it would require the procedural and exemption provisions of the FOI Act to be reproduced in the *Privacy Act*; and

- the Privacy Commissioner's resources would be diverted to complaints about access and amendment to the possible detriment of the other IPPs.[243]

The joint review then considered other suggestions as to how to reduce the overlap between the two pieces of Commonwealth legislation so far as access and amendment rights are concerned.

Firstly, it considered removing the amendment provisions alone from the *FOI Act* to the *Privacy Act*. However, the joint review concluded that because many amendment requests are preceded by access requests this would not be a desirable solution.[244]

Secondly, it considered the approach which is employed in several Canadian provinces; namely, to have joint privacy and access to information legislation. However, the joint review concluded that, given that the Commonwealth already has separate privacy and FOI legislation in place, this would require significant cost and time outlays associated with major agency restructuring.[245]

The joint review concluded that the overlap between the Acts did not give rise to difficulties such that would require a major change in legislative arrangements. Nevertheless, it did make a number of recommendations to facilitate the administration of the relevant provisions relating to access to, and amendment of, personal information.[246] These recommendations included the appointment of an FOI Commissioner responsible for issuing guidelines to assist agencies administer the *FOI Act* (Cth) and who should be required to consult with the Privacy

---

241 This comment is made in the federal Privacy Commissioner's submission to the committee's inquiry, 26 August 1997, pp 13-14.

242 The access and amendment provisions are in IPPs 6 and 7 of the *Privacy Act* (Cth).

243 ALRC/ARC, op cit, p 56, para 5.17.

244 Ibid, p 57, para 5.18.

245 Ibid, p 57, para 5.19.

246 Ibid, pp 57-59, paras 5.21-5.23.

Commissioner before issuing guidelines on access to, and amendment of, personal information. (Queensland already has an Information Commissioner.)[247]

The joint review also noted that it was possible for the Privacy Commissioner to disagree with an agency's decision to refuse to release or to amend an applicant's personal information and that it was unsatisfactory that both the Administrative Appeals Tribunal (AAT) and the Privacy Commissioner may be able to determine the correctness of a decision made under the *FOI Act* (Cth). The joint review concluded that this situation would result in confusion, uncertainty and encourage 'forum shopping'. Therefore, the joint review also recommended that the *Privacy Act* (Cth) should be amended to provide that the Privacy Commissioner cannot find an agency has breached IPP 6 or 7 in respect of a decision made under the *FOI Act* (Cth) unless that decision has been found on external review by the AAT of the federal court to be incorrect.[248]

The joint review's recommendations have not yet been acted upon.

6.6.2.2 Arguments raised in public consultation

The majority of submissions which addressed the issue of the interrelationship of FOI and any privacy legislation to be introduced in Queensland, emphasised that there should be consistency between the two.

The Information Commissioner, Mr Fred Albietz, canvassed in some detail the question of whether the proposed privacy legislation should refer to 'personal information' or should be harmonised with the FOI legislation which refers to 'personal affairs information'. In this regard Mr Albietz referred to relevant case law (which he has endorsed and followed in Queensland) which states that the term 'information concerning a person's personal affairs' is not as broad in scope as the term 'personal information'. Mr Albietz explained:

> *I have interpreted the former term to mean information about the private aspects of a person's life, and it has been established that the term does not extend to information which merely concerns the performance of by a government employee of his or her employment duties (see* Re Pope and Queensland Health *(1994) 1 QAR 616 at pp 658-660). This approach harmonises with the object of promoting greater scrutiny and accountability, in respect of the performance of government functions. In jurisdictions like the Commonwealth of Australia and Western Australia, which have in recent years based their privacy exemption in FOI legislation on the phrase 'personal information', special provision has had to be made in respect of information concerning the performance by a public sector employee of his or her duties of employment.*[249]
>
> *It is important that relevant provisions of the FOI Act and any Queensland privacy statute (the application of which carries the potential to bring the law into disrepute by leading to inconsistent results when applied essentially to identical information) should be brought into harmony as far as practicable.*

Mr Albietz also recognised that there would be an overlap between the current FOI Act and privacy legislation and that it would not be possible to eliminate that overlap by a measure

---

247 Ibid, p 58, rec 16.

248 Ibid, p 59, para 5.23.

249 It will be recalled that the same point was made above by the ALRC and ARC.

such as removing all rights of access to, or amendment of, personal information from the FOI Act into privacy legislation. In this regard Mr Albietz warned that there will always be a fundamental tension between privacy laws and FOI laws and the practical problems of bringing them into harmony should not be underestimated.

Rather than addressing all potential difficulties in his submission, Mr Albietz suggested that his office's experience should be availed of in drafting any new privacy legislation and any consequential amendments to the FOI Act.

The Department of Justice also noted that the term 'personal information' in the *Privacy Act* (Cth) includes more information than 'personal affairs information' in the FOI Act and recommended that its proposed administrative scheme refers to 'personal affairs information'. In addition, the department submitted that access and alteration of documents would be dealt with under the FOI Act and the gathering, use, storage and disclosure of 'personal affairs information' would be dealt with under the administrative privacy scheme.

> *The protection of 'personal information' under an administrative privacy scheme would not restrict the right of access which exists under the Freedom of Information Act 1992 to those documents which do not contain 'personal affairs information'. Clearly, the use of the term 'personal information' in an administrative privacy scheme is untenable. Any other approach would require amendments to the Freedom of Information Act 1992.*[250]

The CJC also considered that the FOI Act should retain provisions dealing with protection (sic) and amendment of personal information and that there be consistency of terminology in both Acts (either 'personal information' or 'personal affairs' with a clear definition of whatever term is used). The CJC also noted that the Commonwealth system, even with the overlap between the FOI and privacy legislation, is not unworkable but that obviously the consequences of any overlap between FOI and privacy legislation would need to be made clear. Thus, it supported a similar approach in relation to separate FOI and privacy legislation in Queensland.

6.6.2.3 Analysis and conclusion

The committee is concerned that as far as possible there should be a workable relationship between Queensland's existing FOI legislation and its proposed privacy legislation. In order to ensure this outcome, careful consideration must be given to two areas:

- firstly, the terminology to be used particularly given the 'personal affairs information' exemption under s 44 of the FOI Act; and
- secondly, the location of the provisions relating to access and amendment of one's own information held by the government.

The first of these issues in essence is whether the term 'personal affairs information' or 'personal information' should be used in Queensland privacy legislation. Section 44 of the FOI Act (the exemption to access provision) and Part 4 of the FOI Act (in relation to amendment of information) use the term 'personal affairs information'. The IPPs in the *Privacy Act* (Cth)

[250] Department of Justice, submission dated July 1997, p 40.

which the committee has recommended be the model for Queensland's IPPs relate to 'personal information'.

It is clear from the case law referred to above that the term 'personal affairs information' is not as broad in scope as 'personal information'.

As some submissions suggest, a simple solution to ensuring harmony between the FOI and privacy legislation would be to use the term 'personal affairs information' in any proposed privacy legislation.

However, the committee is concerned that the use of this term could detract from the effectiveness of a privacy regime. Given that 'personal affairs information' has been interpreted to mean information about the private aspects of a person's life, use of that term in privacy legislation would mean that there could be a substantial amount of other personal information to which it arguably should, but does not, apply. Examples of such information are listed in the above commentary.

Consistent use of the term 'personal information' in both privacy and FOI legislation would also present problems. Information privacy regimes in other jurisdictions, such as the Commonwealth and New Zealand, use the term 'personal information'. However, as the Information Commissioner pointed out, where the term 'personal information' has been used in privacy exemptions in FOI legislation in other jurisdictions, special provision has had to be made to cater for situations in which information should be released in accordance with the tenets of FOI legislation.

Therefore, whilst the committee sees the argument for consistency in terminology it is not convinced that consistency is vital. In order to meet the objectives of both the privacy and the FOI legislation it may be necessary to:

- use the more limited term 'personal affairs information' in relation to third party exemptions from access under the FOI Act; and

- use the term 'personal information' in relation to access and amendment rights of individuals to their own information.

With respect to the location and/or interrelationship of 'access and amendment' provisions, the committee notes that privacy and FOI legislation have interrelated at the Commonwealth level via all applications for access to, and correction of, 'personal information' being dealt with under the FOI legislation. The committee also notes that despite submissions that this situation be changed so that all access and amendment to personal information occur under the *Privacy Act* (Cth), the ALRC and ARC's joint review did not agree that this should occur.

Instead, the joint review recommended that a new FOI Commissioner be responsible for issuing relevant guidelines (after consultation with the federal Privacy Commissioner).

Queensland's *FOI Act* likewise contains extensive provisions dealing with amendment of 'personal affairs information' and therefore it may be possible for those more detailed mechanisms to be utilised rather than replicating them in the Privacy Act (Qld). However, the committee notes the comments of the federal Privacy Commissioner that access to, and amendment of, personal information is essentially a 'privacy' right.

Support for amendment rights to be in privacy legislation is drawn from the *Privacy Act* (NZ), Part V of which contains procedural provisions relating to access to, and correction of, personal information. Moreover, these rights of access and correction have been described as the most significant *privacy* principles for a number of reasons.

> *They have the most tangible effect on protecting personal privacy because they enable individuals to exert practical control over the use of personal information about them. This element of control is a key privacy value. By exercising the rights of access and correction, some of the power to uphold personal privacy reverts to the individual*.[251]

Whilst the committee favours this approach, it is particularly swayed by the comments of the Information Commissioner that the practical problems of bringing FOI and privacy legislation into harmony should not be underestimated. Given all the difficulties noted above, the committee believes that the issue of the interrelationship of the FOI Act with the Privacy Act (Qld) be the subject of detailed consultation with the Information Commissioner in the drafting of the Privacy Act (Qld), but that the committee's comments as above are taken into account in such drafting.

6.6.2.4 Recommendation

Recommendation 10 - The committee recommends that, given the complexity of issues arising in considering the interrelationship between the *Freedom of Information Act 1992* (Qld) and the Privacy Act (Qld), the Information Commissioner be extensively consulted with in the drafting of the Privacy Act (Qld) and any consequential amendments to the *Freedom of Information Act 1992* (Qld).

However, the committee also recommends that, during that process, consideration be given to the committee's points noted above, in particular, the committee's:

- **questioning of the need for there to be consistency in terminology in both pieces of legislation;**
- **suggestion that the effectiveness of a privacy regime might be restricted if its application is confined to 'information concerning a person's personal affairs'; and**
- **discussion regarding the desirability for access and amendment provisions to be, as far as possible, contained in the Privacy Act (Qld).**

6.6.3 Privacy and archives legislation

6.6.3.1 Background

The *Libraries and Archives Act 1988* (Qld) (the L and A Act) aims to promote the making and preservation of public records of Queensland and establishes a right of access to records after the expiration of a restricted access period. Therefore, the introduction of privacy legislation should also be considered in conjunction with certain existing provisions of the L and A Act.

---

[251] Longworth and McBride, op cit, p 89.

The L and A Act establishes Queensland State Archives and gives that body certain functions in relation to 'public records'. 'Public records' are defined in the Act to mean the documentary, photographic, electronic, mechanical or other records of a 'public authority'. A 'public authority' includes departments, boards, commissions, a local government and other institutions of the State.[252]

The functions of State Archives according to the Act are to: promote the making and preservation of the public records of Queensland; to exercise control over their retention and disposal; to provide facilities for their storage and use; and to provide administration in respect of anything stored by it.[253]

State Archives identifies its core activities as:

- identifying public records of enduring value;
- approving the disposal of public records which are no longer required by government for administrative, legal, financial or research purposes; and
- providing access to public records which, at the expiration of a restricted access period, become publicly available for research.[254]

Public records come into the possession of State Archives either as soon as practicable after the expiration of 30 years from the time they were brought into existence, or earlier with the consent of the State Archivist.[255] It is an offence for a person to dispose of public records other than by depositing them with State Archives unless the State Archivist has authorised the disposal or certain other conditions are fulfilled.[256]

There would seem therefore to be two primary areas in which archives and privacy legislation may potentially overlap.

The first of these areas is in relation to access to documents which contain certain personal information. Pursuant to Regulations 21 and 22 of the *Libraries and Archives Regulations 1990* (L and A Regulations), the State Archivist may *generally* permit access to, and inspection by, any person of the 'public records' in the possession of Queensland State Archives after the expiration of 30 years of the date of last dealing. The period during which access to public records is unrestricted is referred to as the 'open access' period.

However, there are some exceptions to this general provision including a restriction on access to personal and staff files of the members, officers and employees of a public authority until the expiration of 65 years after the date of last dealing.[257]

Regulation 23(3) of the L and A Regulations also provides that the Chief Officer of a public authority may impose prohibitions, conditions and restrictions on the access to, and inspection

252 These definitions are contained in s 5 of the Act.
253 s 50(1).
254 As stated in a submission to the committee by Queensland State Archives, Information and Procurement Division, Department of Public Works and Housing, 9 September 1997, p 2.
255 See ss 54 and 57.
256 s 55.
257 See Reg 22(c).

of, public records in the open access period because the public records contain information the disclosure of which:

- is prohibited or restricted by law;
- may be prejudicial to public interest; or
- *may adversely affect the privacy of any person*.

Obviously, many older records contain a great deal of information, some of it personal, which is valuable to researchers. Potentially privacy legislation could restrict, or at least highly regulate, access to records containing personal information in the open access period.[258]

However, at the Commonwealth level this problem does not arise as the IPPs in the *Privacy Act* (Cth) do not apply to information in the 'open access' period as defined by the Commonwealth archives legislation. This is because the definition of 'record' in s 6 of the *Privacy Act* (Cth) states that a 'record' does not include Commonwealth records as defined in the *Archives Act 1983* (Cth) that are in the open access period for the purposes of that Act.

The rationale behind this is explained by the ALRC in its Draft Recommendations Paper 4 on a *Review of the Archives Act 1983* (Cth):

> *At present the Information Privacy Principles contained in the Privacy Act do not apply to records in the open period. Thus access decisions made under the Archives Act do not need to adhere to the Privacy Principles. Application of the Principles to records more than 30 years of age would be overly restrictive. Providing access to records in the open period must take into consideration the fact that sensitivities attaching to information may diminish after 30 years. Preventing the disclosure of all personal information, including names of individuals, would greatly inhibit the provision of open access to archival records*.[259]

Despite this general exemption, privacy is not totally disregarded when making access decisions under the Commonwealth *Archives Act*. Section 33(1)(g) of that Act currently makes exempt from access during the open access period information which, if disclosed, would involve the unreasonable disclosure of information relating to the *personal affairs* of any person (including a deceased person).

In its current review the ALRC has recommended that this exemption be redrafted to be *information relating to personal affairs, the disclosure of which would cause harm to any person*.[260] Notably, the ALRC also considered recommending changing the term 'personal affairs' to 'personal information' to make it consistent with the terminology used in the *Privacy Act* (Cth) and *Freedom of Information Act* (Cth). However, the ALRC concluded that the broader term 'personal information' should not be adopted in the context of the exemption provisions in the archives legislation. According to the ALRC 'personal affairs' *presents a*

---

258 For example, IPP 11 of the *Privacy Act* (Cth) [which the committee has recommended should be adopted in Queensland] provides that a record-keeper who possesses a record that contains personal information shall not disclose that information to a person, body or agency other than the individual concerned subject to certain exceptions.

259 ALRC, DRP 4, *Review of the Archives Act 1983*, Australian Government Printing Service, December 1997, para 15.29.

260 Ibid, p 141, draft recommendation 19.3.

much clearer indication of the type of information which may require protection beyond 30 years.[261]

The ALRC also recommended (in draft) that in relation to this exemption the National Archives of Australia, in consultation with the Privacy Commissioner and relevant responsible agencies, should be required by the legislation to establish and publish guidelines to assist in the administration of the personal affairs exemption category.[262]

Other draft recommendations of the ALRC regarding personal information in the archives context are set out in chapter 20 of its report.

The second area of potential overlap between privacy and archives legislation concerns the disposal of records. As already noted, s 55 of the L and A Act provides that the State Archivist must authorise the disposal of public records. Even if Queensland privacy legislation adopted a similar definition of 'record' as in the *Privacy Act* (Cth), s 55 would apply to records of personal information not in the 'open access' period.

Whilst neither the Commonwealth nor the proposed Queensland privacy legislation give their privacy commissioners powers of disposal, it is feasible that the disposal of records containing personal information by a privacy commissioner could be an issue in some circumstances.

The issue of disposal of records is canvassed briefly in the ALRC's draft recommendations paper. It notes that both Commonwealth FOI and privacy legislation address the rights of 'record subjects' to access records relating to themselves, to seek their amendment, and to be reassured that the information they contain is not misused. However, it is also noted that none specifically address the disposal of such records.[263] Whilst the ALRC does not recommend that archives legislation make specific provision for the disposal of records relating to individuals, it does recommend (in draft) that the Privacy Commissioner in consultation with the National Archives of Australia should consider issues relating to the disposal of records containing personal information with a view to jointly developing appropriate records disposal authorities.[264]

It should also be noted that the federal Privacy Commissioner's February 1998 'National Principles' for the private sector do introduce a disposal principle. Principle 4.2 requires that organisations should take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. Therefore, if in the future a similar principle was adopted in relation to the public sector, disposal may become more of an issue.

6.6.3.2 Arguments raised in public consultation

In its submission Queensland State Archives stated that its principal concern with privacy legislation is that access to public records, which have long been available to researchers under the L and A Act and public records created in the future, may become unavailable to those researchers. In this regard it stressed that sensitivity in records diminishes over time (which any proposed privacy legislation should recognise), and all public records identified as having enduring value should eventually become available for research.

---

261 Ibid, p 141, para 19.16.
262 Ibid, p 143, draft recommendation 19.6.
263 Ibid, p 74, para 10.34.
264 Ibid, p 74, draft recommendation 10.9.

Therefore, State Archives submitted that privacy legislation/guidelines should not apply to records of enduring value in archival custody.

With respect to the disposal of records, State Archives submitted that any future privacy legislation should be consistent with the current archives legislation and that the disposal of public records should remain a function of the Queensland State Archives. Its concern is that destruction may be seen as a way to protect privacy in records.

6.6.3.3 Analysis and conclusion

The committee believes that as far as possible any privacy legislation in Queensland should interrelate with the L and A Act. The relationship between the Commonwealth archives and privacy legislation is somewhat instructive in this regard.

Queensland State Archives' principal concern is that researchers' access to public records which contain personal information and are in the open access period, will be restricted or extinguished by privacy legislation/guidelines.

The question of access to public records in the 'open access' period is not an issue at the Commonwealth level as the IPPs in the *Privacy Act* (Cth) do not apply to records in the 'open access' period as defined by the Commonwealth *Archives Act*. Privacy of information in that open access period is further protected by an exemption regarding access to information relating to the personal affairs of any person.

There would be sound reasons for adopting a similar approach in Queensland. As Queensland State Archives and the ALRC point out, sensitivity in records diminishes over time. There is also a public interest in researchers being able to access historical information, some of which will contain personal information. In these circumstances, the application of IPPs such as those in the *Privacy Act* (Cth) would appear to be overly restrictive. Therefore, the committee believes that the definition of 'record' in the Privacy Act (Qld) should not include a record in the open access period as set out in the regulations to the L and A Act.

If this approach is adopted in Queensland there is still provision under Regulation 23(3) of the L and A Regulations for access to personal information in the 'open access' period to be restricted if it would adversely affect the privacy of any person. However, the committee believes that the terminology used in this section should be amended so as to refer to 'personal affairs information'. It should not be amended to refer to 'personal information'. In this regard, the committee agrees with the ALRC that the narrower term is more consistent with the object of archives legislation.

The second concern of State Archives is with respect to the disposal of public records. This does not seem to be a major issue at this stage given that the committee does not propose that the Queensland Privacy Commissioner/Committee have any powers of disposal, or that the Privacy Act (Qld) advocate disposal as a mean of protecting the privacy of information.[265]

However, given that there may be exceptional cases in which disposal of certain records containing personal information by the Queensland Privacy Commissioner/Committee is an

[265] Although, the committee does recognise that this could be an issue in the future if the February 1998 National Principles do become uniform national principles in relation to both the private and public sectors. This is because these principles currently contain a disposal principle.

issue, the logical approach seems to be that the circumstances in which this occurs should be the subject of protocols between the Queensland Privacy Commissioner/Committee and the Queensland State Archivist. This would in any case seem to tie in with the current procedures for disposal of public records as set out in s 55 of the L and A Act.

A final point that the committee notes is that there are a number of recommendations relating to Queensland's archives legislation which were made by EARC[266] and its Parliamentary Committee[267] but remain outstanding. These bodies recommended that separate archives legislation, dealing with matters such as access to public records in the principal legislation, be enacted in Queensland as soon as practicable. This committee believes that further consideration needs to be given to these recommendations in the short term.

6.6.3.4 Recommendation

Recommendation 11 - The committee recommends that the provisions in the *Libraries and Archives Act 1988* (Qld) should interrelate with the Privacy Act (Qld). Therefore, the committee recommends that:

- **the definition of 'record' in the Privacy Act (Qld) should not include a record in the 'open access' period as currently set out in the regulations to the *Libraries and Archives Act;***
- **the terminology used in the 'privacy' exemption currently contained in regulation 23(3)(c) of the *Libraries and Archives Regulations 1990* should be redefined to relate to 'personal affairs information'; and**
- **any issue relating to the disposal of public records by the Queensland Privacy Commissioner/Committee, should be the subject of disposal protocols between the Queensland Privacy Commissioner/Committee and the Queensland State Archivist.**

The committee further recommends that the responsible Minister review, in the short term, Queensland's archives legislation as proposed by the former Electoral and Administrative Review Commission and the former Parliamentary Committee for Electoral and Administrative Review.

[266] Electoral and Administrative Review Commission, *Report on Review of Archives Legislation*, Queensland Government Printer, Brisbane, June 1992.

[267] Parliamentary Committee for Electoral and Administrative Review, *Archives Legislation*, Queensland Government Printer, Brisbane, November 1992.

7. CHAPTER 7 - A QUEENSLAND PRIVACY COMMISSIONER/ COMMITTEE

7.1 A PRIVACY COMMITTEE OR COMMISSIONER?

7.1.1 Background

The committee has already concluded that a statutory privacy committee or commissioner should be established in Queensland to at least have certain functions in relation to the implementation of IPPs applicable to the handling of personal information by the state's public sector. In this chapter the committee discusses the form that that entity should take.

A number of options exist. For example, Queensland could establish:

- a privacy committee; or
- a privacy commissioner alone; or
- a privacy commissioner assisted by an advisory committee.

Alternatively, the functions of a privacy committee/commissioner could be given to an already existing body or officer such as the Ombudsman, Information Commissioner or Anti-Discrimination Commissioner.[268]

A number of advantages would flow from having a committee as opposed to a single commissioner. These include the fact that, in order to ensure a balanced approach to privacy issues, committee members could be drawn from a variety of backgrounds and industries in which privacy concerns arise. Thus, members could be drawn from both the public and private sectors and from academic institutions, community advocacy and business groups. Members with particular expertise in information technology could also have a significant input.

As already noted in chapter 4, both the New South Wales Privacy Committee and the South Australian Privacy Committee are constituted by members drawn from a wide range of relevant backgrounds.

A privacy commissioner alone would also have certain advantages, not the least of which would be the ability to operate efficiently and without delaying resolution of important matters until a committee could next convene. In the area of complaint resolution and urgent policy advice this is an important consideration.

A third alternative is that which exists at the Commonwealth level. The *Privacy Act* (Cth) establishes both a privacy commissioner and a privacy advisory committee. Part VII of this Act, which relates to the privacy advisory committee, provides that the committee consists of the Privacy Commissioner (who is the convenor of the committee[269]) and not more than 6

[268] The question of the combination of the Queensland Privacy Commissioner with another officer is discussed in more detail in section 7.4 of this report.

[269] s 82(5).

other members who are appointed by the Governor-General on a part-time basis.[270] Of these appointed members:

- at least one must have had at least 5 years' experience at a high level in industry, commerce, public administration or the service of a government or government authority;
- at least one must have had at least 5 years' experience in the trade union movement;
- at least one must have had extensive experience in electronic data-processing;
- at least one shall be appointed to represent general community interests, including interests relating to social welfare; and
- at least one shall be a person who has had extensive experience in the promotion of civil liberties.[271]

However, the Act requires that the Governor-General shall ensure that the majority of appointees are not officers or employees of a Commonwealth authority or instrumentality.[272]

The functions of the advisory committee are:

> · *on its own initiative, or when requested by the Commissioner, to advise the Commissioner on matters relevant to his or her functions;*
>
> · *to recommend material to the Commissioner for inclusion in guidelines to be issued by the Commissioner pursuant to his or her functions; and*
>
> · *subject to any direction given by the Commissioner, to engage in and promote community education, and community consultation, in relation to the protection of individual privacy.*[273]

Meetings of the advisory committee are convened by the Privacy Commissioner as he/she considers necessary for the performance of the committee's functions.[274] In her latest annual report the federal Privacy Commissioner reports that the advisory committee met three times during the year.[275]

The *Privacy Act* (NZ) also establishes an office of the Privacy Commissioner.[276] There is no provision in the Act for a privacy advisory committee. Similarly, the Canadian *Privacy Act* is administered by a single Privacy Commissioner.

---

270 s 82(2)-(3).
271 s 82(7).
272 s 82(6).
273 s 83.
274 See s 87 regarding meetings of the advisory committee.
275 Privacy Commissioner, *Ninth Annual Report 1996-97*, op cit, p 87.
276 s 12.

7.1.2 Arguments raised in public consultation

Of the public submissions that addressed the particular issue of whether there should be a privacy committee or a privacy commissioner, most preferred the establishment of a separate commissioner.

Some of the most compelling evidence in this regard was provided by the Queensland Anti-Discrimination Commission (ADC-Q) which has had experience with being led by a single commissioner. At the Townsville public hearing, Ms Jayne Finlay from the Commission, responded as follows to a question about the advantages of a Commissioner as opposed to a committee.

> *The one really good thing about having the commissioner is that she is very accessible, very easy to get information from and only a phone call away from me. She has made herself very available. That has had some really good benefits. I have had hands-on assistance directly from one person, rather than waiting to get information back. Sometimes you need that information immediately, especially if it is a matter of policy. Having one person there has made that easier. If you had to wait for a committee to meet, it might make it a bit more difficult.*[277]

A number of submissions also recommended that this commissioner be supported by an advisory committee. For example, in its written submission the ADC-Q suggested that the Privacy Commissioner could be assisted by a reference or advisory group to provide specialist advice and a range of views.

The value of an advisory committee was also stressed by the federal Privacy Commissioner in her submission to the committee.

> *If a commissioner were appointed it would be strongly desirable for there to be a formal consultative mechanism to allow advice from those who work within the scheme to flow to the commissioner on a regular basis. The federal Privacy Act established a Privacy Advisory Committee to carry out this role. The membership of an advisory body should be representative of the organisations covered by the scheme and of clients and consumers*[278].

Very few submitters proposed that the functions of a privacy committee/commissioner should be given to an already existing body or officer. This is discussed further in section 7.4 of this report.

7.1.3 Analysis and conclusion

Clearly a privacy commissioner and privacy committee each have their own advantages. The committee has carefully considered each of these advantages and attempted to establish their practical viability by studying the experience in other jurisdictions.

As a result, the committee does have a concern that a privacy committee may be cumbersome in its ability to address issues. The New South Wales Privacy Committee's Annual Report for 1994/95 states that during the reporting period the full committee met on 11 occasions.[279]

---

277 Transcript, 14 November 1997, p 23.

278 Federal Privacy Commissioner, submission dated 26 August 1997, p 6.

279 New South Wales Privacy Committee, *Annual Report 1994/95*, op cit, p 52.

Whilst the committee respects the work and achievements of that committee and its professional secretariat, it does believe that if privacy is to be seriously addressed then there must be a full-time rather than part-time entity to investigate, determine, resolve and consider matters. This is particularly important given that the committee proposes wide functions for this entity, not the least of which is monitoring the implementation of IPPs.

The committee notes that those jurisdictions which have privacy regimes similar to that proposed by the committee for Queensland (that is, the Commonwealth, New Zealand and Canada) have all employed a single commissioner to implement that regime. To the best of the committee's knowledge that has proved a successful model and there have been no proposals for change to a privacy committee.

The ADC-Q's experience with a single commissioner further reinforces that a privacy commissioner as opposed to a committee may be preferable in terms of accessibility and operational efficiency.

However, it is also important that the entity administering any privacy regime is in close consultation with those affected by, or subject to, the regime. In order to promote acceptance of, and compliance with, a regime it must be workable and to a certain extent respond to the concerns of those covered by it. The committee believes that in order to ensure this feedback, there will have to be structured avenues by which such meaningful consultation can take place.

The model which applies at the Commonwealth level, that is, a Privacy Commissioner assisted by an advisory committee would appear to combine both the advantages of a separate privacy commissioner and at the same time maintain an important avenue of advice for the Commissioner. Additionally an advisory committee could, as occurs at the Commonwealth level, engage in and promote community education and consultation in relation to the protection of individuals' privacy.

For these reasons the committee believes that a separate Queensland Privacy Commissioner should be established and that this commissioner should be assisted by a privacy advisory committee. The committee has also considered in some detail the provisions in Part VII of the *Privacy Act* (Cth) and believes that provisions relating to Queensland's privacy advisory committee should be modelled on those provisions.

In particular, the committee believes that:

- the advisory committee should consist of a maximum of seven members which includes the Queensland Privacy Commissioner and six other members who represent organisations covered by the privacy regime and other clients and consumers;

- the functions of the advisory committee should include advising the Queensland Privacy Commissioner on matters relevant to his/her functions, (particularly systemic and policy issues requiring detailed consideration) and, subject to the Queensland Privacy Commissioner's direction, engaging in and promoting community education and consultation in relation to the protection of privacy; and

- meetings of the privacy advisory committee should be convened by the Queensland Privacy Commissioner as she/he considers necessary for the performance of the committee's functions.

7.1.4 Recommendation

Recommendation 12 - The committee recommends that the Privacy Act (Qld) provide for the establishment of a full-time Queensland Privacy Commissioner rather than a Queensland Privacy Committee.

The committee further recommends that the Queensland Privacy Commissioner be assisted by a privacy advisory committee also to be established under the Privacy Act (Qld). The provisions relating to the establishment, constitution and functions of that advisory committee should be broadly modelled on those contained in Part VII of the *Privacy Act 1988* (Cth).

7.2 THE QUEENSLAND PRIVACY COMMISSIONER'S FUNCTIONS

7.2.1 Background

Thus far in this report the committee has concluded that at the very least the Queensland Privacy Commissioner should have certain functions in relation to monitoring compliance with the IPPs as set out in the Privacy Act (Qld). Foreseeably this would include: receiving and investigating complaints about breaches of the IPPs; conducting audits of compliance with the IPPs; providing guidance as to the interpretation of the IPPs; making recommendations as to any amendments that may need to be made to the IPPs; and conducting education and consultation in relation to the operation of the IPPs.

However, one would also expect the Queensland Privacy Commissioner, as an integral part of an information privacy regime, to have broader functions in relation to protecting the information privacy of individuals. These broader function should include certain reporting functions and ensuring that due regard is given to individuals' privacy in any proposed legislation.

The functions of the federal Privacy Commissioner as they relate to general privacy protection are contained in s 27 of the *Privacy Act* (Cth).[280] In summary these functions include:

- investigating alleged breaches of the IPPs by agencies and where appropriate attempting to settle the matters giving rise to such investigations by conciliation [s 27(1)(a)];
- examining (with or without a Minister's request) proposed enactments which may have an adverse effect on the privacy of individuals [s 27(1)(b)];
- researching and monitoring developments in computer technology and data processing to ensure that any adverse effects of such developments on the privacy of individuals are minimised and to report to the Minister thereon [s 27(1)(c)];
- promoting an understanding and acceptance of the IPPs and their objects [s 27(1)(d)];
- preparing and publishing guidelines for the avoidance of acts or practices that might

[280] In chapter 11 of this report the committee discusses the Queensland Privacy Commissioner's functions beyond information privacy and, in particular, whether these s 27 functions should apply only to information privacy.

have an adverse effect on the privacy of individuals [s 27(1)(e)];

- providing advice (with or without a request) to a Minister or an agency on any matter relevant to the operation of the Act [s 27(1)(f)];
- maintaining and publishing annually a Personal Information Digest being a compilation of the matters set out in records maintained by record-keepers in accordance with clause 3 of IPP 5 [s 27(1)(g)];
- conducting audits of records of personal information maintained by agencies for the purpose of ascertaining whether the records are maintained according to the IPPs [s 27(1)(h)];
- informing the Minister of action that needs to be taken by an agency in order to achieve compliance with the IPPs [s 27(1)(j)];
- examining (with or without a request from a Minister) proposals for data matching or data linkage that may have an adverse impact on the privacy of individuals [s 27(1)(k)];
- undertaking educational programs for the purpose of promoting the protection of individuals' privacy [s 27(1)(m)];
- encouraging corporations to develop programs for the handling of records of personal information that are consistent with the OECD Guidelines [s 27(1)(n)];
- doing anything incidental or conducive to the performance of any of the preceding functions [s 27(1)(o)];
- issuing guidelines under provisions of certain legislation [s 27(1)(p) & (pa)];
- monitoring and reporting on the adequacy of equipment and user safeguards [s 27(1)(q)]; and
- reporting to the Minister (with or without a request) in relation to any matter that concerns the need for, or the desirability of, legislative or administrative action in the interests of privacy of individuals [s 27(1)(r)].

Section 29 of the *Privacy Act* also provides that in performing his or her functions and powers under the Act, the federal Privacy Commissioner shall have regard to certain matters including:

- the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way; and
- international obligations accepted by Australia, including those concerning the international technology of communications and developing general international guidelines relevant to the better protection of individual privacy.

More specific provisions relating to certain powers of the federal Privacy Commissioner are also contained in the *Privacy Act* (Cth). These include:

- Part IV, Division 3 which deals with reports by the Commissioner;
- Part V which deals with matters including investigations of complaints, investigations on the Commissioner's initiative and determinations following investigation of complaints; and
- Part VI which deals with the Commissioner's ability to make public interest determinations about certain acts and practices. (The committee has already recommended in section 6.4 of this report that the Queensland Privacy Commissioner have a similar ability.)

Part IV, Division 3 and Part V of the *Privacy Act* (Cth) are canvassed in more detail in the following section which deals with the Queensland Privacy Commissioner's powers.

It is also instructive to refer to those provisions of the New Zealand *Privacy Act* which relate to the New Zealand Privacy Commissioner's functions.[281] Whilst broadly these provisions are similar to those contained in the *Privacy Act* (Cth) some notable differences include functions in relation to monitoring the use of unique identifiers and monitoring compliance with the public register privacy principles.[282]

7.2.2 Arguments raised in public consultation

The federal Privacy Commissioner's submission stressed that three essential functions of a privacy commissioner are conducting education, monitoring technological trends, and receiving and handling complaints.

Many other submissions agreed that these were essential functions of a privacy commissioner. Other important ancillary functions noted in the submissions included:

- auditing records of personal information maintained by organisations covered by the regime to establish whether systems are in place which are consistent with the privacy principles;
- determining any exceptions to the regime's application where the public interest favours such an exception;[283]
- determining compensation for citizens whose privacy the commissioner has determined has been unreasonably breached and imposing penalties;[284]
- monitoring charging regimes to ensure that they remain reasonable and in line with the intent of the legislation;
- conciliating between citizens whose privacy the commissioner has determined has been unreasonably breached;

---

281 These functions are contained in s 13 of the Act.

282 The definition of 'unique identifiers' and public register privacy principles are briefly canvassed in chapter 6 of this report.

283 The issue of exceptions and the Queensland Privacy Commissioner's functions in this regard are canvassed in section 6.4 of this report.

284 The question of determining compensation and imposing penalties is dealt with in more detail in the following section of this report.

- recommending and preparing subordinate legislation with respect to privacy issues; and

- reporting to Parliament on at least an annual basis as to the matters the subject of the commissioner's functions.[285]

Notably, the Department of Justice recommended slightly different functions for the Queensland Privacy Commissioner given its proposal that at first instance the Office of the Privacy Commissioner be established and that that officer then submit to Cabinet principles to be approved for the protection of privacy of personal information. In essence, the department submitted that the functions of the Queensland Privacy Commissioner should be:

- ensuring the protection of information privacy via the development of principles (including exemptions) for the protection of information held by the state government departments and agencies;

- receiving and investigating complaints and making reports on non-compliance with the privacy regime in a similar fashion to the Ombudsman;

- educating and informing state government departments and agencies of their responsibilities for privacy protection;

- once the privacy principles are promulgated as a cabinet administrative instruction, publishing guidelines to assist departments and agencies to avoid acts or practices that may have an adverse effect on the privacy of individuals;

- inquiring generally into any matter covered by the Privacy Commissioner Bill proposed by the department;

- reporting, *at the request of the responsible Minister*, on the need for or desirability of taking action to improve the privacy of individuals that may be infringed by state government departments and agencies; and

- conducting audits, *when requested by a department or agency*, of records of personal information maintained by state government departments and agencies for the purposes of ascertaining whether the records are maintained according to the privacy principles once issued.

The CJC also proposed a number of functions for the Queensland Privacy Commissioner in the context of law enforcement agencies. These included the oversight of: the destruction of fingerprints; use of surveillance devices; and use of telephone interception powers.

However, as Dr Brereton from the CJC acknowledged at the committee's seminar on privacy, the CJC's submission was written prior to the passing of some recent significant criminal justice and law enforcement legislation in Queensland. This legislation includes *the Criminal Justice Act Amending Legislation Act 1997*, the *Police Powers and Responsibilities Act 1997* and the *Queensland Crime Commission Act 1997*.[286]

[285] The question of annual reporting is dealt with further in section 9.3 of this report.

[286] Transcript, 17 November 1997, p 6.

The Telecommunications (Interception) Queensland Bill 1998 was also introduced into the Queensland Legislative Assembly on 5 March 1998. This Bill will enable the Queensland Police Service (QPS), the Queensland Crime Commission (QCC) and the Criminal Justice Commission (CJC) to use telecommunications interception as an investigative tool for certain serious offences. The legislation does this by establishing a recording, reporting and inspection regime to complement the Commonwealth *Telecommunications (Interception) Act 1979*.

In so far as the CJC's submission related to the functions of a Queensland Privacy Commissioner, Dr Brereton noted that this recent legislation introduced some new bodies responsible for monitoring the use of certain powers by law enforcement agencies. These bodies included a Parliamentary Commissioner and a 'public interest monitor'. The Commonwealth Ombudsman will also be involved in monitoring the use of the power to intercept telecommunications.

The CJC's view, as expressed by Dr Brereton, is that it is undesirable to have so many different bodies involved in overseeing and monitoring the activities of law enforcement agencies. The CJC's concerns in this regard relate to the likelihood of duplication, the difficulty in maintaining a consistent approach to issues of privacy regulation and the heightened danger of some privacy related matters 'falling between the cracks'.[287]

Therefore, according to Dr Brereton, the CJC believes that if a Queensland Privacy Commissioner is to be established serious consideration will have to be given to how the commissioner 'fits in' with these other monitoring bodies. The CJC did not believe that it would be appropriate to exclude law enforcement agencies from the Queensland Privacy Commissioner's jurisdiction given that privacy issues are particularly relevant in the area of law enforcement. Instead, the CJC's preferred approach is that the Queensland Privacy Commissioner would take over the responsibilities of these other bodies at least in so far as they relate to privacy issues. Although the CJC recognised that this would be a difficult task, it submitted that the approach would reduce the risk of duplication and maximise consistency.[288]

7.2.3 Analysis and conclusion

As the foregoing discussion illustrates, the Queensland Privacy Commissioner can have a wide range of functions. Some of these functions have already been addressed in this report. For example, the committee has already recommended in chapter 6 that the Queensland Privacy Commissioner should have the ability to issue codes of practice modifying the application of the IPPs and to determine 'public interest' exemptions to the IPPs.

However, clearly there is a need for Queensland privacy legislation to identify the primary functions of the Queensland Privacy Commissioner. The CJC also highlighted in consultation that the commissioner may have other functions in relation to overseeing law enforcement agencies with respect to privacy issues.

A study of comparative privacy legislation together with the comments made in submissions supports the notion that the key functions of the Queensland Privacy Commissioner should, with respect to individuals' information privacy, be:

- receiving, investigating and conciliating complaints by individuals that an act or

[287] Ibid, p 7.
[288] Ibid.

practice of an agency may be in breach of an IPP;

- ensuring compliance with the IPPs via conducting audits of agencies covered by the regime, providing advice to both agencies and their responsible Ministers, and preparing and publishing guidelines;

- monitoring technological trends and making recommendations with respect to any amendments that should be made to the regime or any proposed enactments which may have an adverse affect on the privacy of individuals;

- generally promoting an acceptance of the IPPs and conducting education with respect to privacy; and

- reporting with respect to the above matters either with or without a request.

The committee agrees with this approach. In order for a privacy regime to be effective it must be administered by a entity with appropriate functions. These functions must be designed to ensure compliance with the regime and provide means by which individuals can enforce their rights. In the case of the latter, this means that an individual must be able to have access to an independent entity who can receive and impartially investigate an allegation that an agency has engaged in an act or practice which interferes with their privacy.

Moreover, it is highly desirable that there be systems in place to ensure that technology is monitored for potential breaches of privacy, and that the law generally keeps abreast of this technology. The Queensland Privacy Commissioner would be the most appropriate entity to ensure that this important task is effectively fulfilled.

The committee also sees a key role for the Queensland Privacy Commissioner in promoting an understanding and acceptance of the privacy regime and promoting the protection of individuals' privacy generally. Central to changing attitudes or developing a privacy 'culture' (whether of agencies or the community in general) is education. The importance of educating people with respect to privacy was stated by the federal Privacy Commissioner in her submission.

> *Education and persuasion designed to change cultures and increasing sensitivity to privacy issues has a crucial part to play in promoting respect for individuals' privacy rights.*[289]

The Queensland Privacy Commissioner should also have a number of other functions which to some extent supplement these core functions. These functions also appear in s 27 of the *Privacy Act* (Cth). For example, the committee believes that the Queensland Privacy Commissioner should have the ability to issue guidelines with respect to interpretation of the IPPs. The federal Privacy Commissioner currently issues guidelines pursuant to s 27(1)(d) of the *Privacy Act* (Cth) which states that it is a function of the Commissioner 'to promote an understanding and acceptance of the Information Privacy Principles and of the objects of those Principles'. The New Zealand Privacy Commissioner has a similar function under s 13(1)(a) of the *Privacy Act* (NZ).

[289] Federal Privacy Commissioner, submission dated 26 August 1997, p 9.

Whilst the guidelines issued by the federal Privacy Commissioner are of no force and relate only to policy, they do provide important direction to agencies in attempting to ensure compliance with the Act.

Therefore, the committee concludes that the functions of the Queensland Privacy Commissioner should be broadly modelled on those contained in s 27 of the *Privacy Act* (Cth) as they incorporate both the key and supplementary functions that it sees as necessary for any privacy commissioner. These functions should also be broad enough to permit the Queensland Privacy Commissioner to attend to matters such as establishing any necessary protocols between jurisdictions in the area of privacy. (For example, if state and federal schemes are going to cover some of the same organisations it would be sensible for the Commissioner to look at establishing co-operative arrangements to prevent forum shopping and to simplify administration.)

However, the committee makes the following observations with respect to the application of the functions listed in s 27 to Queensland.

Firstly, the committee has some reservation as to whether the Queensland Privacy Commissioner should be obliged to maintain and publish annually a Personal Information Digest. The time and cost involved in preparing such a digest should be carefully considered given that under clause 3 of IPP 5 a record-keeper is obliged to maintain a record setting out certain details as to records they keep and that under clause 4 of that IPP a record-keeper is to make that record available for inspection by members of the public.

In this regard, it is noted that the New Zealand Privacy Commissioner has the *discretion* from time to time to publish one or more publications that include matters concerning personal information held by an agency.[290]

Secondly, whilst the matter of to whom the Queensland Privacy Commissioner should account is discussed in detail later in this chapter, it is relevant to note at this stage that the committee believes that, in general, the Queensland Privacy Commissioner should be accountable to Parliament. This should therefore be taken into account when modelling the Queensland Privacy Commissioner's functions on those contained in s 27, particularly s 27(1)(c) and s 27(1)(r). (For example, reports to the Minister under those provisions should also be furnished to a relevant Parliamentary committee.) However, for the avoidance of doubt, the committee does stress that this should not in any way prevent a Minister from requesting the Queensland Privacy Commissioner to conduct research, examine a proposed enactment or provide advice regarding privacy issues.

For reasons directly related to the Commissioner's independence and accountability, the committee does not agree that the Queensland Privacy Commissioner should only be able to undertake certain functions at the Minister's request as proposed by the Department of Justice. Suffice to say at this stage that, as the Queensland Privacy Commissioner will be primarily monitoring and investigating complaints against state government departments and agencies, he/she must not be, or be seen to be, subject to direction or control by the Executive arm of government. In order to ensure this independence, the Queensland Privacy Commissioner must be able to conduct investigations and audits, and prepare reports as she/he sees fit.

[290] Refer to s 13(1)(d) and s 21.

It is also relevant to note that s 27 of the *Privacy Act* (Cth) allows the federal Privacy Commissioner to perform many of his/her functions with or without a request from a Minister.

A final point in relation to the Queensland Privacy Commissioner's general functions relates to s 29 of the *Privacy Act* (Cth). This provision requires the federal Privacy Commissioner to have regard to certain matters in exercising his/her functions and powers under that Act. Relevantly these include the protection of important human rights and social interests that complete with privacy including the desirability of the free flow of information and certain rights of government and business to achieve their objectives in an efficient way. Further, the federal Privacy Commissioner is to take account of relevant international obligations and guidelines.

The committee believes that s 29 is an important provision. As noted at the outset of this report, privacy protection is in essence a question of appropriately balancing competing interests. Section 29 ensures that the federal Privacy Commissioner is, by statute, required to consider that balance.

Further, the importance of Australia's international obligations with respect to privacy has also already been noted. Due regard to such obligations and documents has a different meaning at the state rather than Commonwealth level, although their impact is a matter in relation to which any state privacy commissioner should be informed.

Therefore, the committee also believes that a provision modelled on s 29 of the *Privacy Act* (Cth) should be contained in the Privacy Act (Qld).

Functions in relation law enforcement agencies

A final area to be addressed in relation to the Queensland Privacy Commissioner's functions, is in relation to law enforcement agencies. The committee agrees with the comments made by Dr Brereton of the CJC as to the desirability for consistency and lack of duplication in the monitoring of Queensland's law enforcement agencies with respect to privacy issues. Therefore, careful and detailed consideration needs to be given to how the functions of the Queensland Privacy Commissioner will interrelate with the functions of other persons and bodies such as the Parliamentary Criminal Justice Commissioner and Public Interest Monitor.

The committee also agrees with the CJC's preferred position that the Queensland Privacy Commissioner take over the responsibilities of these other bodies in so far as they relate to privacy issues. This would avoid the possibility of duplication and ensure a more consistent approach to issues of privacy regulation. However, as noted by Dr Brereton, realigning the responsibilities of the different bodies and persons with these responsibilities will be a complex task.

There would appear to be little merit in such a complex task being undertaken prior to confirmation of the establishment of a Queensland Privacy Commissioner. Therefore, the committee believes that a more appropriate and sensible approach would be for the matter to be considered and reported upon by the Queensland Privacy Commissioner as a matter of priority upon that officer's appointment.

Other functions

Addressed later in this report are other functions/powers of the Queensland Privacy Commissioner relating to:

- investigating complaints regarding privacy;
- reporting both generally and on an annual basis;
- privacy in the broader 'public sector' and the private sector; and
- other specific information and non-information privacy concerns.

7.2.4 Recommendation

Recommendation 13 - The committee recommends that the functions of the Queensland Privacy Commissioner should be broadly modelled on the functions of the federal Privacy Commissioner as set out in s 27 of the *Privacy Act 1988* (Cth).[291] However, the committee recommends that these functions should be adapted to reflect that:

- **the Queensland Privacy Commissioner has a discretion to annually publish a Personal Information Digest as required by the equivalent of s 27(1)(g) of the *Privacy Act* (Cth); and**
- **for the purposes of the functions contained in the equivalent of s 27(1)(c) and (r) of the *Privacy Act* (Cth), the Queensland Privacy Commissioner is required to report to the Minister and to Parliament.**

The committee further recommends that:

- **a provision modelled on s 29 of the *Privacy Act 1988* (Cth) be contained in the Privacy Act (Qld); and**
- **the Queensland Privacy Commissioner should be primarily responsible for monitoring Queensland's law enforcement agencies with respect to privacy issues given the desirability for consistency and lack of duplication in this regard. However, this matter is to be further considered and reported upon by the Queensland Privacy Commissioner as a matter of priority upon that officer's appointment.**

7.3 THE QUEENSLAND PRIVACY COMMISSIONER'S POWERS

7.3.1 Background

In order to carry out his/her functions effectively and efficiently the Queensland Privacy Commissioner must be given appropriate powers. This is particularly so in relation to his/her functions associated with receiving and investigating complaints, where foreseeably powers

[291] These functions are in addition to the other functions for the Commissioner already outlined, that is, issuing codes of practice and making public interest determinations.

that the Commissioner would need include powers of access, production, attendance and determination.

However, a certain balance must also be achieved in determining powers that are to be conferred on the Commissioner. On the one hand, the ability to exercise coercive powers should not detract from the overall aim of the regime which is to promote the protection of individuals' privacy. On the other hand, the regime must be, and be seen to be, capable of enforcement in order to gain the respect of those subject to it.

Again the Commonwealth *Privacy Act* is instructive with respect to what powers the Commissioner may need in this regard.

General powers

Section 27(2) provides that the federal Privacy Commissioner has the power to do all things that are necessary or convenient to be done for or in connection with the performance of his or her functions under s 27(1).

In addition, s 68 provides that for the purposes of the federal Privacy Commissioner performing his or her functions under the *Privacy Act* (Cth), a person authorised by the federal Privacy Commissioner is empowered to enter premises occupied by an agency and inspect any documents that are kept at those premises and that are relevant to the performance of those functions. Such entry is conditional on either consent of the occupier of the premises, or authorisation pursuant to a warrant issued under the Act.[292]

Therefore, for example, this power may be used in fulfilment of the Commissioner's function to conduct audits of records of personal information maintained by agencies for the purposes of ascertaining whether the records are being maintained in accordance with the IPPs. [This function is pursuant to the equivalent of s 27(1)(h) of the *Privacy Act* (Cth).]

Powers relating to the investigation of complaints

Part V of the *Privacy Act* (Cth) which deals with the investigation of complaints and investigations on the Commissioner's initiative, also contains a number of powers.

Pursuant to s 36 an individual may complain to the federal Privacy Commissioner about an act or practice that may be an interference with the privacy of the individual and the Commissioner is obliged to investigate such a complaint.[293] Pursuant to s 40(2) the federal Privacy Commissioner may also investigate an act or practice if it may be an interference with the privacy of an individual and the Commissioner thinks its is desirable that the act or practice be investigated.

Part V also sets out the federal Privacy Commissioner's powers as part of investigating such complaints. These powers include the power to:

- decide not to investigate a complaint in cases such as where the complaint is frivolous, vexatious, misconceived or lacking in substance;[294]

[292] s 68(3).
[293] s40(1) obliges the Commissioner to investigate such complaints.
[294] s 41(1)(2) and (4).

- defer an investigation in certain circumstances;[295]
- conduct preliminary inquiries in order to determine whether he/she has the power to investigate the matter or whether he/she will decide not to investigate the matter;[296]
- for the purposes of an investigation, obtain information from such persons, and make such inquiries, as he/she thinks fit;[297]
- give a person believed to have information or a document relevant to an investigation, a written notice requiring the person to give the information or produce the document to the Commissioner, or to attend before the Commissioner to answer questions relevant to the investigation[298] (the Commissioner may examine a person attending before him/her on oath or affirmation[299]);
- (for the purposes of performing the Commissioner's functions in relation to a complaint), direct by written notice the complainant, respondent and any other person likely to be able to provide information or assist in relation to the complaint to attend a conference presided by the Commissioner;[300]
- require a person attending a conference to produce a document;[301] and
- transfer a complaint to a more appropriate body for investigation.[302]

Following investigation of a complaint, the Commissioner has the power to either make a determination dismissing the complaint, or find the complaint substantiated and make a determination that includes one or more of the following:

- a declaration that the respondent has engaged in conduct constituting an interference with the privacy of an individual and should not repeat or continue such conduct;
- a declaration that the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;
- a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint; or
- a declaration that it would be inappropriate for any further action to be taken in the matter.[303]

---

295 s 41(3).
296 s 42.
297 s 43(3).
298 s 44(1) and (3).
299 s 45.
300 s 46. Failure to attend is an offence punishable, in the case of an individual, by a fine not exceeding $1 000 or imprisonment for a period not exceeding 6 months (or both) and in the case of a body corporate a fine not exceeding $5 000. Offences to be contained in the Privacy Act (Qld) are discussed in chapter 9 of this report.
301 s 47.
302 s 50.
303 s 52. Loss or damage in these declarations includes injury to the complainant's feelings or humiliation suffered by the complainant. s 52(1A).

In making a determination either dismissing or substantiating a complaint, the Commissioner may also include a declaration that a complainant is entitled to a specified amount by way of reimbursement of expenses reasonable incurred with the making and investigation of the complaint.[304]

Such determinations by the Commissioner are not binding or conclusive between any of the parties to the determination.[305] However, as a result of the Commissioner's determinations, certain obligations fall on the agency (under s 58) or the principal executive of the agency (under s 59) whichever is applicable.[306] If an agency or the principal executive of an agency fails to comply with s 58 or s 59 then the Commissioner or a complainant can apply to the Federal Court for an order directing compliance.[307]

A complainant can also apply to the Administrative Appeals Tribunal (AAT) for a review of:

- a declaration in which the complainant is awarded compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint; or
- a decision of the Commissioner refusing to include such a declaration in a determination.[308]

Reporting powers

The above paragraphs discussed the powers of the Queensland Privacy Commissioner in relation to investigating complaints and making *determinations* following those investigations. Another important role proposed for the Queensland Privacy Commissioner is the Commissioner's 'Ombudsman-like' function to inquire into government practices that impact on individual's privacy and make *recommendations* and report in relation to them.

Such powers could be based on the federal Privacy Commissioner's reporting powers. These powers are outlined in Part IV, Division 3 of the Privacy Act and relate to reporting:

- following the Commissioner's investigation of an act or practice (including investigations conducted on the Commissioner's own motion);
- following the Commissioner's examination of a proposed enactment;
- following the Commissioner's monitoring of certain activities or conducting an audit.

Whilst these reports are to the Minister, there is also provision for certain reports to be tabled in Parliament.[309]

The offence provisions which relate to a failure by persons to comply with a lawful exercise of power by the federal Privacy Commissioner are canvassed in section 9.4 of this report.

The *Privacy Act* (NZ) grants the New Zealand Privacy Commissioner similar powers to the federal Privacy Commissioner.[310]

---

304 s 52(3).
305 s 52(1B).
306 ss 57-59.
307 s 62.
308 ss 61.
309 Reports are tabled in Parliament in accordance with s 30(5), s 31(5) and s 32(3).

7.3.2 Arguments raised in public consultation

The federal Privacy Commissioner again made some instructive comments in her submission regarding any powers that the committee may consider conferring on the Queensland Privacy Commissioner. At the outset the Commissioner highlighted to the committee the need to approach the question of coercive powers with caution.

> *The primary objective of a Privacy Commissioner or privacy committee is to promote respect for individual privacy. The amount of emphasis placed on measures like fines, disciplinary actions and the exercise of coercive powers should accord with the contribution they can make to this goal.*

In this context the Commissioner stressed that many privacy concerns arise more because policy makers and administrators lack an appreciation of the implications of their actions rather than because they wilfully ignore privacy concerns. Therefore, that office's experience has been that education and promoting cultural change in the relevant agencies has been more effective in changing behaviour than threatening punitive action.

However, the federal Privacy Commissioner recognised that whilst the powers available to the office have rarely been used, the fact that they exist has assisted in "getting agencies to take privacy protection seriously". Information provided in the Commissioner's submission revealed that only two formal determinations have been made by the federal Privacy Commissioner and only one of these awarded some financial compensation. Further, the Commissioner advised that a large number of other complaints have been conciliated with settlement payments of up to $22 000, although the average payment is apparently much smaller.

The federal Privacy Commissioner also advised the committee that two powers are particularly important to the effective functioning of a privacy commissioner, namely:

- the power to initiate investigations on his/her own motion which allows the Commissioner to be pro-active and means that issues can be addressed as they emerge rather than as complaints are received; and

- the power to audit entities covered by the privacy regime which has proved important in achieving systematic change within government agencies via the highlighting of areas for improvement and providing a robust framework for monitoring agency responses.

The necessity for appropriate powers to back the functions of a Queensland Privacy Commissioner was stressed in a number of other submissions. For example, the QCCL stated:

> *The Privacy Committee/Commissioner should have the appropriate powers necessary to enforce the functions of the Committee/Commissioner, which should include the enforcement of IPPs. Without enforcement powers, balanced of course against the rights of individuals in particular circumstances, any protection of privacy would be completely inadequate. There is, in QCCL's view, absolutely no point in establishing a Committee/Commissioner which has no teeth to enforce legislation however wide*

[310] See generally Part VIII of the *Privacy Act 1993* (NZ).

> *ranging it may be*.[311]

The remainder of public submissions which specifically canvassed the question of the Privacy Committee/Commissioner's powers generally agreed that such powers should include the powers necessary to:

- receive, investigate, conciliate, hear, and determine complaints;
- audit entities covered by the regime; and
- enforce IPPs through sanctions such as fines or disciplinary action (the Australian Privacy Charter Council thought that this fine should be in the form of compensation to complainants who have suffered loss as a result of actions contravening the legislation).

Some submissions expressed the view that caution should be exercised in relation to the power of access as it has the potential to itself invade the privacy of citizens. Whilst it was recognised that access is necessary and appropriate to undertake privacy audits, access for the purposes of conducting investigations was seen as a matter perhaps requiring the Privacy Commissioner to be issued with a warrant.

The Criminal Justice Commission noted in this regard:

> *If the Commissioner is to investigate complaints of breaches of privacy, he or she must be granted rights of access to agency or departmental records to determine: whether a breach has occurred; if information has been disseminated to others, to whom and what information has been disseminated; whether the breach was inadvertent or deliberate; whether the processes of the agency which breached an individual's privacy are inadequate*.[312]

The CJC went on to recommend that powers of access, at least as wide as those in the current *Privacy Act* (Cth), be granted to the person or body responsible for dealing with complaints of breaches of privacy principles. The CJC further submitted that if the Commonwealth model is found too restrictive, the alternative model in the *Criminal Justice Act* may be adopted. This Act allows a CJC officer (authorised in writing by the Chairperson) to enter and search the premises of a 'unit of public administration' when a Supreme Court judge has authorised the issue of a warrant.

The Department of Justice also agreed that the Queensland Privacy Commissioner would need certain coercive powers. However, the department did not favour the use of the federal Privacy Commissioner's powers as a model. Rather, the Department submitted that the Privacy Commissioner have all the powers, rights and privileges that are specified in the *Commission of Inquiry Act 1950*, a model which is used for both the Queensland Ombudsman and the New South Wales Privacy Commissioner.

7.3.3 Analysis and conclusion

The committee agrees with comments to the effect that coercive powers should not be conferred on any officer or entity without sufficient justification and that, in the case of the

311 Queensland Council for Civil Liberties, submission dated 12 August 1997, p 9.
312 Criminal Justice Commission, submission dated 12 August 1997, p 6.

Queensland Privacy Commissioner, these powers should not detract from the primary goal of promoting good privacy practices in relation to individuals' personal information.

However, the committee also believes that in order for the Queensland Privacy Commissioner to be an effective privacy watchdog the Commissioner must have the powers necessary to enforce compliance with the regime that he/she is responsible for administering.

The committee therefore agrees with the majority of submissions that the Queensland Privacy Commissioner should be conferred those powers necessary to give effect to the Commissioner's statutory functions.

These powers will need to include a general power of access and inspection necessary for the Queensland Privacy Commissioner to fulfil functions such as his/her audit function. As submissions to the committee revealed, this audit function is seen to be an important responsibility of the Queensland Privacy Commissioner and must be accompanied by powers necessary to give effect to it.

In this regard the committee has considered the power granted to the federal Privacy Commissioner pursuant to s 68 of the *Privacy Act* (Cth), particularly in light of the concerns raised in some submissions regarding the power of access. As it currently stands, the power of entry and inspection in s 68 is subject to consent of the occupier or the issue of a warrant. The committee believes that these restrictions on the power are appropriate and should adequately address the concerns expressed in some submissions that there does need to be appropriate limits on the power of access.

In relation to the investigation of complaints, the committee believes that the Queensland Privacy Commissioner should not only be able to receive complaints from individuals about privacy, but also have the power to conduct on his/her own motion an investigation into an act or practice of an agency and the power to report on those investigations. This would not only enhance the independence of the Queensland Privacy Commissioner but would also allow the Commissioner to be pro-active in addressing identified areas of concern.

Additional powers that the Queensland Privacy Commissioner will need in relation to his/her function to receive, investigate, conciliate, hear, and determine complaints against agencies should include:

- the power to determine not to investigate a complaint on the basis that it is frivolous, vexatious, misconceived or lacking in substance, or to defer investigation of a complaint;
- powers of production, attendance and questioning;
- the power to conduct compulsory conferences; and
- the power to transfer complaints to more appropriate bodies.

Some of these powers will also be necessary in cases where the Commissioner conducts investigations on his/her own motion.

After investigation of a complaint the Queensland Privacy Commissioner must also have the power to make appropriate determinations or declarations. The committee believes that the type of determinations that the Queensland Privacy Commissioner should be empowered to

make should be the same as those available to the federal Privacy Commissioner; namely, determinations that:

- the complaint is unsubstantiated and therefore dismissed;
- the complaint is substantiated and therefore a declaration that:
  - the respondent has engaged in conduct which is in breach of the privacy of an individual and should not be repeated or continued;
  - the respondent should perform a certain act to redress any loss or damage suffered by the complainant;
  - the complainant is entitled to a specified amount by way of compensation as a result of the act which is the subject of the complaint; or
  - it would be inappropriate for any further action to be taken in the matter.

In the case of both powers of investigation and determination, the committee has carefully considered the powers granted to the federal Privacy Commissioner under Part V of the *Privacy Act* (Cth). The committee believes that they represent a conferral of power that is appropriate and necessary to enable the Privacy Commissioner to perform his/her functions. Therefore, the committee endorses those general powers as a model on which the Queensland Privacy Commissioner's powers should be based.

However, appropriate modifications would have to be made in relation to the enforcement provisions currently contained in the *Privacy Act* (Cth). Consideration also needs to be given to the appeals mechanisms open to complainants.

As noted above, s 61 of the *Privacy Act* (Cth) provides that applications can be made to the AAT for merits review[313] of certain declarations and decisions made by the Privacy Commissioner regarding compensation. Currently Queensland does not have a general merits review body equivalent to the AAT, although recommendations have been made previously by the Electoral and Administrative Review Commission (EARC)[314] and the Parliamentary Committee for Electoral and Administrative Review (PCEAR)[315] for the creation of such a generalist merits review body in Queensland in order to rationalise the current system of external review of administrative decisions.

One option open to the committee is to recommend the creation of a separate tribunal to hear appeals from decisions of the Queensland Privacy Commissioner. Another option open to the committee is to confer on an existing review body additional jurisdiction to review matters determined by the Queensland Privacy Commissioner. In this regard the committee notes that

313 Merits review is where a challenge to a decision is resolved through the reviewer standing in the shoes of the original decision maker, looking afresh at the merits of the case and deciding whether the original decision was the correct or preferable one, given all the circumstances of the case. Merits review is to be contrasted with judicial review. Under the *Judicial Review Act 1991*, the focus of the challenge is primarily on the legality of how the original decision was made. The subject of inquiry is whether the decision-maker acted within his/her lawful power.

314 Electoral and Administrative Review Commission, *Report on Review of Appeals from Administrative Decisions*, Queensland Government Printer, Brisbane, August 1993.

315 Parliamentary Committee for Electoral and Administrative Review, *Report on Review of Appeals from Administrative Decisions*, Queensland Government Printer, Brisbane, May 1995.

under the *Privacy Act* (NZ) aggrieved individuals can bring proceedings before the Complaints Review Tribunal.[316]

Given EARC's and the PCEAR's comments regarding the need to restrict the on-going ad hoc proliferation of review tribunals which has resulted in the disjointed treatment of merits review in Queensland, the committee is hesitant about recommending the creation of another separate tribunal. However, by the same token, the committee believes that the decisions of the Queensland Privacy Commissioner should not be final and that there must be some avenue for merits review of the Privacy Commissioner's decisions. In determining which tribunal should have this jurisdiction, further consideration may need be given to acting upon the former recommendations of EARC and PCEAR.

The Queensland Privacy Commissioner should also be subject to judicial review under the *Judicial Review Act 1991* (Qld).[317]

A final but important issue to be considered is the 'Ombudsman-like' reporting powers that the Queensland Privacy Commissioner should have. In order to be truly effective the Commissioner must be able to report on a range of matters of concern so that any remedial or other action can be taken. Therefore, like the federal Privacy Commissioner, the Queensland Privacy Commissioner must have the ability to report:

- following the investigation of an act or practice (including an investigation conducted on the Commissioner's own motion);
- following the examination of a proposed enactment; and
- following the monitoring of certain activities or conducting an audit.

However, whilst the committee again believes that the *Privacy Act* (Cth) is a broad model to be followed in drafting these reporting power provisions, the committee does recommend that a number of matters be clarified. In particular, the committee believes that the Commissioner's reporting powers should be drafted widely enough to permit the Commissioner to report on any matter within his/her jurisdiction at any time. Further, on the basis of maintaining the Commissioner's independence, the committee believes that relevant reports by the Commissioner should be furnished to both the Minister and to Parliament.[318]

In concluding that the Queensland Privacy Commissioner's powers should be modelled on those in the *Privacy Act* (Cth), the committee has given careful consideration to the Department of Justice's submission that the Queensland Privacy Commissioner should have all the rights powers and privileges in the *Commissions of Inquiry Act 1950* (Qld). However, the committee does not believe that this is the more appropriate course in this case given that:

---

316 See ss 82-85 of the *Privacy Act* (NZ). The Complaints Review Tribunal was constituted by s 45 of the *Human Rights Commission Act 1977* (NZ) and is continued by s 93 of the *Human Rights 1993* (NZ). The Tribunal primarily considers proceedings brought under the discrimination provisions of the *Human Rights Act* and the complaints provisions under the *Privacy Act*.

317 Further consideration will also have to be given to enforcement of decisions of the Privacy Commissioner that relate to private sector service providers. (The committee, in chapter 8, recommends that the proposed privacy regime apply to certain private sector service providers.)

318 The committee's reasons in this regard are explained more fully in section 7.5 of this report. The issue of annual reporting by the Queensland Privacy Commissioner is also canvassed in section 9.3.2 of this report.

- the committee has already recommended wider functions for the Queensland Privacy Commissioner than those recommended by the Department of Justice; and

- the committee believes that powers modelled on the federal Privacy Commissioner's powers are more appropriate because they are more privacy specific.

In section 9.5 of this report the committee canvasses the offence provisions that should apply if the Queensland Privacy Commissioner is obstructed in the exercise of his/her functions or powers.

7.3.4 Recommendation

Recommendation 14 - The committee recommends that the Privacy Act (Qld) confer on the Queensland Privacy Commissioner the powers necessary to effectively and efficiently fulfil the Commissioner's functions under that proposed legislation including in particular:

- **the power of access and entry to premises occupied by an agency either with consent of the occupier or by warrant;**

- **the power to initiate his/her own investigation in relation to an act or practice of an agency that may constitute an interference with the privacy of an individual;**

- **powers in relation to the investigation of complaints lodged by individuals including powers of determination and declaration (regarding matters such as compensation); and**

- **reporting powers.**

Further, the committee recommends that these powers be broadly modelled on those powers available to the federal Privacy Commissioner under the *Privacy Act 1988* (Cth), subject to the following considerations.

Firstly, the committee recommends that appropriate amendments be made in relation to appeal and review mechanisms open to complainants. These amendments should reflect that decisions of the Queensland Privacy Commissioner are subject to both judicial review under the *Judicial Review Act 1991* (Qld) and merits review. The Committee recommends that, in determining which merits tribunal should hear matters brought under the Privacy Act (Qld), the Queensland government give further consideration to acting upon the recommendations of the former Electoral and Administrative Review Commission and the former Parliamentary Committee for Electoral and Administrative Review in this regard.

Secondly, the committee recommends that the reporting powers of the Queensland Privacy Commissioner be broadly drafted so as to permit the Commissioner to report in relation to any matter within his/her jurisdiction as the Commissioner sees fit. Relevant reports should be furnished both to the Minister and the Parliament.

7.4 THE COMBINATION OF THE OFFICE OF THE QUEENSLAND PRIVACY COMMISSIONER WITH ANOTHER OFFICE

7.4.1 Background

In a number of jurisdictions the office of the Privacy Commissioner is, or it is suggested should be, combined with another office such as that of the Information Commissioner, Ombudsman or Anti-Discrimination Commissioner. As already noted, in New South Wales indications are that the office of the Privacy Commissioner will be merged with the Anti-Discrimination Board.

At the Commonwealth level the federal Privacy Commissioner's office currently forms a branch of the Human Rights and Equal Opportunity Commission (HREOC). Although, as part of the recent announcement by the Commonwealth government to replace the HREOC with a new body to be called the Human Rights and Responsibilities Commission, the role of the federal Privacy Commissioner will be separated from the Commission and established as a statutory Office of the Privacy Commissioner.[319]

In some Canadian provinces FOI and privacy is dealt with under a single piece of legislation and is administered by an Information and Privacy Commissioner.[320] At the federal level in Canada there is separate privacy legislation, the *Privacy Act*. However, pursuant to this Act the Governor in Council may appoint the Information Commissioner as Privacy Commissioner.[321]

During its study tour to Canada the committee took the opportunity to investigate 'first-hand' the practical operation of combined Information and Privacy Commissioner offices.[322]

The committee was informed by the Canadian Privacy Commissioner, Mr Bruce Phillips, that in 1983 the Canadian FOI and Privacy Offices were established simultaneously and conjointly as, it was thought at the time, that the two offices would deal with essentially 'flip sides of the same coin'. The current Commissioner believes that experience has subsequently shown, however, that the two offices have not a great deal to do with each other: access to information is an administrative right while privacy, at least in Canada, is a constitutional right.

The Commissioner suggested to the committee that, if Queensland should introduce privacy legislation, then the privacy office should not be amalgamated with any FOI office.[323]

The issue of combining the offices of a privacy and Information Commissioner was also considered by the ARC and ALRC in their joint report titled *Open Government: a review of the federal Freedom of Information Act 1982*.[324] In that report the joint review recommended that a new statutory office of FOI Commissioner (Cth) be established and consideration was therefore given as to whether this role could be combined with that of the Commonwealth Privacy Commissioner with perhaps two deputies: one each for privacy and FOI.

---

319 Refer to the press release of the federal Attorney-General and Minister for Justice, the Hon Daryl Williams of 23 September 1997.

320 This occurs for example in the provinces of Ontario and British Columbia.

321 See s 55 of the *Privacy Act* (Canada).

322 See LCARC, 1997, op cit, pp 26-27.

323 Committee meeting with the Privacy Commissioner of Canada, 8 April 1997.

324 ALRC/ARC, op cit.

The joint review noted that a combined position operates in several Canadian provinces and that the approach was attractive in so far as it would require a single person to resolve any tensions between FOI and privacy. However, in conclusion the joint review did not favour this approach as:

- different powers were proposed for the FOI Commissioner from those which the Privacy Commissioner enjoys;
- it was noted that the *Privacy Act* (Cth) may be extended to cover the private sector (and the review did not support the extension of the *FOI Act* to the private sector); and
- it saw the need for there to be *identifiable and unambiguous advocates* for the separate principles of openness and privacy, the absence of which may lead to allegations of bias in favour of one or the other.[325]

Therefore, the joint review concluded that it was not preferable for the role of the Privacy Commissioner to be so extended. The then federal Privacy Commissioner also agreed with this conclusion.[326]

The joint review did however consider that given the connections between FOI and privacy legislation and the review's recommendations for close liaison between the FOI and Privacy Commissioners and between the FOI Commissioner and the Ombudsman, there may be advantages in locating those three offices at the same premises. The review considered that this would not only result in financial savings (through the sharing of corporate support and secretariat services) but would also be convenient for consumers.[327]

Whilst the role of a FOI Commissioner under the Commonwealth FOI system would differ from his/her Queensland counterpart, the above observations are still largely relevant to the matter under current consideration.

7.4.2 Arguments raised in public consultation

Clearly, the majority position expressed on this point in submissions to the committee was that the functions of the Queensland Privacy Commissioner should not be combined with either that of the Information Commissioner or any other office such as the Anti-Discrimination Commissioner. In particular, there was opposition to the Information Commissioner also performing the role of the Privacy Commissioner given the fundamentally different focus and priorities on which each regime is based.

The Information Commissioner also expressed the view that it may be more appropriate to have a separate Office of the Privacy Commissioner.

There was, however, some support for there to be a sharing of administrative services between the Privacy Commissioner and some other office, such as the Office of the Information Commissioner, in order to reduce the costs associated with establishing a new office.

325 Ibid, p 77.
326 Ibid, p 78.
327 Ibid, p 78.

The CJC summarised the general position as follows:

> *In view of the different focus of a Privacy Committee or Commissioner on the one hand, and the Information Commissioner on the other, it may not be appropriate to combine the two offices. The former is concerned with ensuring maintenance of privacy of personal information, whereas the other is focused on having information (in some instances, including personal information) released into, what is in effect, the public arena, unless there are good reasons for not doing so. However, the CJC acknowledges that there could be administrative efficiencies from combining the two functions in the one office.*[328]

7.4.3 Analysis and conclusion

The committee's experience in Canada, together with a study of the observations made in public submissions and the joint report of the ALRC/ARC, provides no sound reason as to why the statutory office of the Queensland Privacy Commissioner should be combined with that of any other office.

The committee notes that some jurisdictions have combined the office of their Privacy Commissioner with that of their FOI Commissioner. However, this is generally where these offices are administering joint privacy and FOI legislation.

The committee does not believe that a combined FOI and privacy office is appropriate given the different focus of the regimes administered by each. The committee fears that it would be difficult for an Information Commissioner to be an impartial advocate for openness of government one day and an advocate for privacy the next. As the joint review of the ALRC and ARC noted:

> *It is particularly important that the benefits of openness, not only for public accountability but for creativity and commercial exploitation, not be diminished by an overemphasis on privacy. Given the tendency to date for agencies to favour secretiveness over openness and the fact that the overwhelming majority of FOI requests are for applicants' personal information, there is a risk that FOI would become the 'poor cousin' if the Privacy Commissioner were given responsibility for the role of FOI Commissioner.* [329]

It is also important that the focus of the Queensland Privacy Commissioner should not be detracted from by that officer having other significant responsibilities such as that required of the Ombudsman or the Anti-Discrimination Commissioner.

However, the committee recognises that there may be significant cost savings realised if the administrative and corporate support provided to the office of the Queensland Privacy Commissioner is shared with that of another office such as the Information Commissioner or Ombudsman.

7.4.4 Recommendation

Recommendation 15 - The committee recommends that the functions of the Queensland Privacy Commissioner should not be conferred on, or combined with, any other office.

---

328 Criminal Justice Commission, submission dated 12 August 1997, p 4.

329 ALRC/ARC, op cit, pp 77-78.

However, the committee accepts that for administrative efficiency, the administrative and corporate support provided to the Office of the Queensland Privacy Commissioner could be shared with another office.

7.5 THE INDEPENDENCE OF THE QUEENSLAND PRIVACY COMMISSIONER

7.5.1 Background

Given that the Queensland Privacy Commissioner will be performing a 'watchdog' role over the public sector in terms of privacy issues, an important consideration is the degree of independence that she/he should have from the Executive arm of government. The investigation of privacy complaints against state government departments and agencies by another agency of the executive conceivably will not be seen to be fair and/or independent.

Comments have also already been made as to the necessity for there to be few restrictions on the way in which the Commissioner can perform his/her functions or exercise his/her powers. In particular, the committee has noted that the Commissioner must be able to conduct privacy-related investigations on his/her own initiative, and report on the performance of his/her functions to both the Minister and to Parliament.

The issue of the Queensland Privacy Commissioner's independence is also relevant in relation to:

- the Commissioner's appointment;
- the manner in which the Commissioner's budget is formulated and reviewed (as an office which is not properly resourced is hampered in its effectiveness); and
- who the Commissioner is generally able/required to report to.

The federal Privacy Commissioner is appointed by the Governor-General[330] and generally reports to the Minister. Although, there is provision for some of the federal Privacy Commissioner's reports (including annual reports) to be thereafter tabled by the Minister in Parliament.[331] Further, under the current structure, the federal Privacy Commissioner receives funds necessary for the performance of his/her functions as part of a single allocation to the HREOC.

Making the Queensland Privacy Commissioner an officer of the Parliament could largely overcome concerns with respect to that officer's independence.

Canada's federal Privacy Commissioner is an independent officer of Parliament appointed by the Governor in Council after approval by resolution of the Senate and House of Commons.[332] The Privacy Commissioner reports to Parliament annually on the activities of his/her office during that year and may, at any time, make a special report to Parliament on any matter within the scope of his/her powers, duties and functions where a matter is of such urgency or importance that it cannot wait until the next annual report.[333]

In addition:

330 s 19 of the *Privacy Act* (Cth).
331 See s 27, ss 30-32 and s 97 of the *Privacy Act* (Cth) in relation to annual reports.
332 See s 53 of the *Privacy Act* (Canada).
333 See ss 38-39 of the *Privacy Act* (Canada).

- the 'administration' of the Canadian *Privacy Act* is required to be reviewed on a permanent basis by such committee of the House of Commons, of the Senate or of both Houses of Parliament as may be designated or established by Parliament for that purpose;[334] and

- the head of every government institution is required to prepare for submission to Parliament an annual report on the administration of the *Privacy Act* within the institution during each financial year. Every report once tabled is referred to the above Parliamentary committee.[335] (Annual reporting by 'agencies' coved by the proposed privacy regime for Queensland is canvassed further in chapter 9 of this report).

In New Zealand, the Privacy Commissioner is appointed by the Governor-General on the recommendation of the Minister of Justice, and the Minister presents the Privacy Commissioner's annual reports to Parliament.[336] However, the status of this office has come under criticism on the basis that whilst it confers an independent status on the Commissioner, that independence may be limited by the fact that the Commissioner is appointed on the recommendation of a member of the Executive. Some believe that given the possibility that the Commissioner may come into conflict with the government of the day, is it to be regretted that the Commissioner was not given the additional independence of being an officer of Parliament.[337]

In fact, a number of submissions concerning the then Privacy of Information Bill 1991 (NZ) argued that the New Zealand Privacy Commissioner should be an officer of the Parliament and, as a result, the Justice and Law Reform Committee further considered this issue. That committee concluded that it would not be appropriate for the New Zealand Privacy Commissioner to be an officer of the Parliament, as the functions of that officer were closer in nature to bodies such as the Human Rights Commission than to Parliamentary officers such as the Ombudsman.[338]

In Queensland the Auditor-General and the Parliamentary Commissioner for Administrative Investigations (the Ombudsman) both have functions relating to the review of government processes. The Ombudsman investigates administrative action taken by or on behalf of government departments and agencies, whilst the Auditor-General monitors the government's financial management. The independence of these officers is secured by virtue of their appointment as officers of the Parliament. Moreover, their accountability to the Parliament is via the Public Accounts Committee[339] and the Legal, Constitutional and Administrative Review Committee[340] respectively.

In relation to both of these officers of the Parliament, their parliamentary committees have responsibilities in relation to:

- their appointment and removal;

- the development of budgets for their offices (a budget developed entirely by Executive processes could also potentially undermine their independence); and

---

334 s 75.
335 s 72.
336 See s 12 and s 24.
337 See Longworth and McBride, op cit, pp 39-40.
338 Ibid, pp 40-41.
339 The relevant provisions are contained in the *Financial Administration and Audit Act 1977* (Qld).
340 The relevant provisions are contained in the *Parliamentary Commissioner Act 1974* (Qld).

- strategic reviews of their offices. (Strategic reviews are basically five-yearly reviews of the performance, management and structure of the office. The conduct of these review are specifically canvassed in chapter 9 of this report.)

Similar processes could be adopted in relation to the Queensland Privacy Commissioner if he/she was to be an independent officer of the Parliament.

7.5.2 Arguments raised in public consultation

The federal Privacy Commissioner submitted that the question of the independence of a Privacy Commissioner is a difficult subject on the following basis.

> *In relation to regulation of the public sector, there is likely to be a trade off between the independence of a commissioner and his or her access to the deliberations of government.*
>
> *The more independent a commissioner is and the more frank and fearless his or her public statements, the more cautious will Ministers and agencies be in involving the commissioner in the development of new proposals that may have privacy implications. Yet it is at the developmental stage that input from a privacy perspective may have the most impact on the eventual outcomes.*
>
> *On the other hand, a commissioner too close to or dependent upon Ministers runs the risk of be co-opted as a legitimator of whatever policies the government and its agencies choose to pursue.*
>
> *The federal Privacy Commissioner has tried to strike a balance between the two extremes. For example, the Commissioner has been prepared to give the government confidential advice on policy proposals and has referred to the relevant Minister requests from the Opposition to see that advice. On the other hand, the Privacy Act provides that the Commissioner's annual report to the Attorney-General must be tabled in parliament and the Commissioner has sometimes used this document as a means of expressing concerns about aspects of government policy.*[341]

However, in terms of accountability the federal Privacy Commissioner also commented:

> *Internationally, a number of jurisdictions have a Privacy Commissioner who is appointed by or reports to Parliament rather than a Minister. These include the German Federal Commissioner for Data Protection and the Canadian Privacy Commissioner. Such a structure would certainly work to ensure greater independence of the Commissioner from the government of the day. It would appear to be an option worth serious consideration.*[342]

A substantial number of submissions specifically supported the notion that a Queensland Privacy Commissioner should be independent and that he/she should be accountable to Parliament. There was also a high level of support for this accountability to be via a parliamentary committee, such as occurs with the Ombudsman.

As stated by the QCCL:

---

341 Federal Privacy Commissioner, submission dated 26 August 1997, p 8.

342 Ibid, pp 8-9.

> *It is clear that a Privacy Commissioner or Committee requires a significant degree of independence from government, but should also be answerable to an appropriate parliamentary committee (such as the Legal, Constitutional and Administrative Review Committee). It needs to be adequately funded, but given that it will have significant investigative and auditing functions with respect to government and semi-government entities, the accountability mechanism should be directed to the Queensland Parliament through a parliamentary committee.*[343]

Ensuring independence via budget allocation was also seen as an important issue by the Criminal Justice Commission.

> *To achieve the independence of the Commissioner—both in reality and in perception—there must be a fair and independent process for budget allocation. The CJC suggests adoption of a process similar to that currently applicable to the Parliamentary Commissioner for Administrative Investigations. This would involve submission of a budget to a Minister, but with that submission being treated separately to the departmental bid and listed separately in the budget papers. The CJC suggests that the proposed Privacy Commissioner be entitled to report directly to Parliament.*[344]

7.5.3 Analysis and conclusion

The committee is concerned that the Queensland Privacy Commissioner, as the entity responsible for administering and enforcing a privacy regime applicable to agencies of the Queensland government should be, and be seen to be, able to carry out his/her functions independent from the Executive arm of government.

Therefore, the committee agrees with the majority of public submissions that the most appropriate way in which the independence of the Queensland Privacy Commissioner can be ensured is via his/her independent status as an officer of the Parliament. As such, the Queensland Privacy Commissioner should be generally required to report to Parliament in the case of both annual and other reports.[345]

The committee has considered the federal Privacy Commissioner's observation that this may mean that departments will be more cautious in involving the Commissioner at the developmental stage of new proposals which might have privacy implications. However, the committee believes that to a large extent the question of the Commissioner's involvement in such proposals is more a matter of the particular Commissioner's operational style than a question of his/her independence.

The committee has had the benefit of assessing the accountability of officers of Parliament through its role in relation to the Ombudsman. From this experience, the committee also supports the notion of a parliamentary committee having certain responsibilities in relation to the Queensland Privacy Commissioner.

---

343 Queensland Council for Civil Liberties, submission dated 12 August 1997, p 8.

344 Criminal Justice Commission, submission dated 12 August 1997, p 4.

345 Annual reporting is dealt with in more detail in section 9.3 of this report. Other reports by the Queensland Privacy Commissioner would be in accordance with his/her functions and powers detailed in sections 7.2 and 7.3 of this report.

The committee believes that at least this parliamentary committee should have two responsibilities.

Firstly, the parliamentary committee should be consulted in relation to the appointment/suspension and removal of the Queensland Privacy Commissioner. This process will ensure that the appointment and removal of the Privacy Commissioner is conducted with bi-partisan input from an arm of government separate to the Executive.

Secondly, the parliamentary committee should be consulted in relation to the formulation of the budget of the Queensland Privacy Commissioner. Such a requirement means that the independence of that officer is further enhanced. A Privacy Commissioner which relies solely on the Executive for funding would in effect be dependent for resources on the arm of government that it oversees.

In its submission the CJC observed the need to ensure the independence of the Commissioner via budget allocation. The PCJC made similar comments in relation to the budget process of the CJC in Report No. 38 *A report on the accountability of the CJC to the PCJC*.[346]

Given its statutory areas of responsibility the committee believes that the appropriate parliamentary committee to undertake these roles in relation to the Queensland Privacy Commissioner is the Legal, Constitutional and Administrative Review Committee.

The committee also believes that for consistency, the provisions in the Privacy Act (Qld) relating to appointment and budget formulation of the Queensland Privacy Commissioner should be modelled on those currently contained in the *Parliamentary Commissioner Act 1974* (Qld).

However, the committee makes this comment subject to one proviso. At the time of writing this report, the inaugural strategic review of the Ombudsman's office is being conducted. Foreseeably, the issue of the formulation of the Ombudsman's budget may be the subject of discussion as part of that review. Therefore, the committee believes that any changes it may recommend to the manner in which the Ombudsman's budget is formulated as a result of this current review, should also be applied in the case of the Queensland Privacy Commissioner.

The committee also believes that the Queensland Privacy Commissioner's Parliamentary committee should be involved in any periodic strategic and other reviews of the Commissioner's office. The conduct of such reviews is canvassed in more detail in section 9.4 of this report.

7.5.4 Recommendation

Recommendation 16 - The committee recommends that the Queensland Privacy Commissioner be an independent officer of the Parliament, accountable to the Queensland Legislative Assembly through the Legal, Constitutional and Administrative Review Committee.

The committee further recommends that the Privacy Act (Qld) provide that the Legal, Constitutional and Administrative Review Committee should be:

[346] Parliamentary Criminal Justice Committee, Report No. 38, Queensland Government Printer, Brisbane, pp 66-69.

- **consulted in relation to the appointment, suspension and removal of the Queensland Privacy Commissioner; and**

- **consulted in relation to the formulation of the budget of the Queensland Privacy Commissioner.**

The relevant provisions in this regard should be modelled on those contained in the *Parliamentary Commissioner Act 1974* (Qld). However, the committee makes this recommendation subject to any changes that it may propose to the provisions in that Act in response to the inaugural strategic review of the Ombudsman's office which is currently being conducted.

8. CHAPTER 8 - THE SCOPE OF THE PRIVACY ACT (QLD)

8.1 INTRODUCTION

In chapters 5 and 6 of this report, the committee recognised that there are strong reasons for consistency between privacy regimes applying to the public and private sectors based on the fact that increasingly the boundary between the private and public sector is becoming less distinct. This breakdown in demarcation is particularly being brought about by the corporatisation and outsourcing of services formerly provided by governments.

In those earlier chapters the committee also discussed the federal Privacy Commissioner's current process in relation to information privacy in the private sector, which may ultimately result in national consistency in information privacy regimes applicable to all Australian public and private sectors.

However, until such time as that may occur, there is an immediate need to address the application of the Privacy Act (Qld) to service providers contracted with by the Queensland government and to public sector enterprises (government owned corporations). There is also a need to consider the application of the proposed legislation to local governments.

8.2 THE APPLICATION OF THE PRIVACY ACT (QLD) TO LOCAL GOVERNMENTS

8.2.1 Background

Many proponents of an information privacy regime for state government departments and agencies also argue that such a regime should logically extend to local governments.

Local governments possess a large amount of personal information about ratepayers and businesses operating within their jurisdiction and, during the course of its inquiry, the committee received a number of submissions alleging a lack of privacy protection afforded to that information. The federal Privacy Commissioner also advised the committee that a considerable number of the general inquires she receives via her office's 'Privacy Hotline' relate to local government matters such as the secondary use of information about building approvals and dog licences.

A particular concern with respect to local governments and privacy is the question of public access to land records and other registers and lists held by them. Section 591 of the *Local Government Act 1993* (Qld) (the 'LG Act') provides that a 'land record' is open to inspection free of charge to owners, lessees or occupiers of land and adjoining land, and to other persons upon the payment of a fee decided by the local government. Regulation 29 of the *Local Government Regulations 1994* provides that a government's 'land record' must contain certain information for each parcel of rateable land in its area. This information includes the owner's name and postal address, the land's size and description, details of the land's value (unimproved and effective value), information about rates for the parcel (including type, amount levied, overdue rates and accrued interest thereon) and any other information that local government considers appropriate.

Local governments also keep other information such as that associated with building applications and approvals.[347] Apparently, the practice of selling 'building approval lists' to third persons for marketing purposes has been common among local governments for some time.

There are obvious cases in which persons will want to seek information about a particular parcel of land. For example, prospective purchasers and mortgagees will want to ensure that all structures on land in which they may potentially have an interest have the requisite building approvals. They will also most probably want to determine whether there are any outstanding rates in relation to the land. However, in accordance with s 591, many local authorities also provide land record updates to third parties such as real estate agents, certain retailers and community organisations who use that information for other purposes such as marketing.

A number of councils have informed the committee that they do receive complaints from persons claiming that they have received 'junk' mail after their names were secured from information provided by their Council through land record updates. The former Queensland Privacy Committee also noted in its Sixth Annual report that it had received a number of complaints regarding the sale of information by local government bodies. In particular, these complaints concerned the sale of information in relation to building applications.[348]

In addition to the needs of prospective purchasers and the like, there would appear to be two other main arguments against extending the application of a privacy regime to local governments. The first of these is cost, both in terms of compliance costs and the loss of revenue collected by local governments from persons inspecting land records.

The second argument is that there should be some access to this information for genuine commercial reasons. In other words, if certain information is publicly available to commercial bodies, it allows marketing to be more targeted. This not only reduces marketing expenditure, but also decreases the waste and nuisance value in providing marketing material to those who are not within the 'target group' for the goods or services in question.

8.2.2 Arguments raised in public consultation

The majority of submissions which addressed this issue supported the extension of an information privacy regime to local governments.

As the QCCL noted:

> *Local government activities are in QCCL's view clearly part of the government sector, and should be subject to exactly the same privacy regulation as State Government activities. There has been a disturbing trend in recent years for Local Government bodies to sell vast amounts of information which they compulsorily acquire, to the extent where the sale of that information (almost inevitably without the specific informed consent of the rate payers concerned) now forms a significant component of the budget of many such Local Government bodies. Local Government is in fact the level of government which most closely touches on the lives of individuals, and therefore clearly requires the application of a privacy protection*

[347] Section 30A of the *Building Act 1975* (Qld) provides that a person shall not carry out building work in respect of which the Standard Building Law requires the approval of the local government unless such approval has been first obtained.

[348] Queensland Privacy Committee, *Sixth Annual Report*, op cit, p 4.

> *regime as much as any other sector, be it public or private.*[349]

Some local authorities themselves recognised the need for more formal regulation in relation to the personal information they collect and hold. For example, the Redland Shire Council submitted:

> *"Information Privacy Principles" enshrined in an act would certainly assist local governments in the protection and use of information in their possession.*[350]

Redland Shire Council further submitted that if local governments were required under their legislation to report on privacy issues in their annual reports, this would further emphasise the importance of promoting the protection of privacy in local government, and serve as a monitoring mechanism by insisting that local governments are aware of the necessity to protect information in their possession.

The committee also heard evidence at its Gold Coast public hearing from Mr Philip Spencer of the Logan City Council (LCC) that, in that council's experience, a code of conduct governing matters including privacy is not the solution to addressing privacy issues as it is not enforceable.

Some councils have taken action with respect to increasing the level of privacy protection offered to their ratepayers. For example, Mr Stevens from the Gold Coast City Council (GCCC) advised the committee at its Gold Coast hearing that, following an investigation by the Ombudsman into a complaint by a person that the sale of building application information to a third person was an invasion of privacy, the GCCC resolved to include on its building application form a box which asks people whether they consent to certain personal information appearing in the council's statistical list of building approvals (that is, an 'opt out' provision).

At the same public hearing, Mr Philip Spencer from the LCC also suggested that access to land records could be further tightened so that councils only made the information available to those who were directly affected by the information that they are seeking.

This comment ties in with the CJC's caution in its written submission that it may not be appropriate to make a blanket decision concerning the application of privacy regulation to local government bodies.

> *For example, many local government activities, such as property ownership records, outstanding rates etc. are currently readily available and frequently obtained in property conveyancing; it would probably be impractical to impose restrictions on access to this material.*[351]

Likewise, the Australian Privacy Charter Council stated that privacy regulation should generally apply to local government activities but that some specific provision may be appropriate in relation to particular organisations. The Council suggested that these should, in general, be catered for through codes, although in a few cases it may be appropriate to address them in the legislation.

---

349 Queensland Council for Civil Liberties, submission dated 12 August 1997, p 11.

350 Redland Shire Council, submission dated 8 August 1997, p 2.

351 Criminal Justice Commission, submission dated 12 August 1997, p 6.

The TCLS also pointed out that it would be anomalous for the FOI Act to apply to information held by councils while privacy legislation did not.

One of the issues raised in the committee's issues paper was whether the costs associated with privacy regulation of local government activities would outweigh the public benefit to be gained by that regulation. Most submitters which felt competent to answer that question (including some local authorities) did so in the negative.

At its Gold Coast public hearing, Mr Spencer of the LCC canvassed the issue of costs that would be incurred if a privacy regime such as that which operates under the *Privacy Act* (Cth) were introduced in relation to local government activities in Queensland. Mr Spencer advised the committee that whilst the council has not looked at costs in detail, it does operate very comprehensive records management systems and that he did not see that there would be a great deal of additional cost from their perspective to maintain that information.

8.2.3 Analysis and conclusion

Clearly, local governments collect and use a significant amount of information about their ratepayers (the majority of which ratepayers are obliged to provide) and, as the evidence above indicates, a number of information privacy concerns arise as a result. In particular, many of these concerns flow from the sale of information (including personal information such as names and addresses) from the land record as currently permitted by the LG Act, and from the sale of building approval lists. The above evidence indicates that some local governments themselves recognise these concerns and would welcome legislative guidance to assist them in the protection and use of personal information in their possession.

On this basis, it is difficult to argue that the broad information privacy principles which the committee has recommended to apply to state public sector departments and agencies should not equally apply to local governments.

Further, for the same reasons as apply in relation to information privacy protection in the state public sector, the committee does not see that cost would outweigh the benefit of this occurring, particularly if there was an adequate phase-in period. The length of this phase-in period should correlate with that afforded to state public sector departments and agencies. Evidence received by the committee as to the cost of privacy regulation for local governments indicated that cost should not be a major factor.

The committee also agrees with the TCLS that it would be anomalous for FOI but not privacy legislation to apply to local governments.

However, the committee does recognise that there may have to some particular consideration given to the provision of certain personal information by local authorities to third persons in some situations.[352]

As noted by the CJC, it would, for example, be necessary for certain information to be available to prospective purchasers in the conduct of searches for property transactions. In some cases this will not be a problem if it involves access to a 'generally available publication'. (This is on the basis that the Queensland Privacy Act adopts the Commonwealth definition of

[352] The extent of such an exception may to some extent depend on whether the privacy regime is to apply to 'personal information' or information concerning a person's 'personal affairs'.

'record' as it does not include a 'generally available publication'). In other cases, the disclosure of this information may fall within one of the exceptions to the IPP concerning disclosure (IPP 11), most likely on the basis that 'the disclosure is required or authorised by or under law'. Should the exceptions contained in the IPPs themselves not be adequate, then the committee has already made recommendations with respect to two other avenues that could be utilised to overcome these concerns.

Firstly, the committee has already recommended that in certain circumstances the Queensland Privacy Commissioner should have the power to issue codes of practice modifying the application of the IPPs to any specified class of information, agency, activity or industry, profession, calling or class.

The provision of certain information to, for example, prospective purchasers and mortgagees may be one such class of information in relation to which a code could be issued. The application of such a code of course would then apply to the provision of that type of information by both local governments and state government departments and agencies.

Secondly, the committee has also recommended that in certain circumstances the Queensland Privacy Commissioner should have the ability to grant public interest exemptions from compliance with the IPPs. There may be situations that arise in the local government or general 'land' searching context which justify such exemptions.

The committee also finds merit in the suggestion that local governments could be required to report on privacy issues in their annual reports as a means of promoting privacy in local government and as a monitoring mechanism. The committee's comments and recommendations regarding annual reporting by agencies is canvassed further in section 9.3.1 of this report.

8.2.4 Recommendation

Recommendation 17 - The committee recommends that the Privacy Act (Qld) apply to local governments.

8.3 THE APPLICATION OF THE PRIVACY ACT (QLD) TO GOVERNMENT CONTRACTORS

8.3.1 Background

Increasingly, government departments and agencies are contracting private sector persons and organisations to perform services which they would traditionally or otherwise provide. (This contracting out of services is also called 'out-sourcing'). At the committee's Gold Coast public hearing it heard that a significant part of local government business is also contracted out.[353]

Should the same or similar privacy legislation as applies to the public sector apply to the private sector, then the application of a privacy regime to these service providers is not an issue. However, if the private sector is not so covered, then the question arises as to the application of a privacy regime to these persons or organisations.

[353] See the evidence of Mr Stevens from the Gold Coast public hearing, Transcript, 7 November 1997, p 30.

In its submission to Victoria's DPAC, the ALRC listed certain reasons as to why companies contracted by government agencies should be subject to a privacy protection regime. The ALRC's observations included:

- service providers hold personal information regarding users of that service that is highly sensitive in nature, regardless of whether that information is released by a government agency or by a company in receipt of government funding, the effect of inappropriate use of that funding is the same;

- user/consumer rights are now a fundamental part of government policy and so it is reasonable to expect that organisations receiving government funding will be required to respect and implement that policy. There should not be any distinction in the privacy rights of service users based on the nature of the entity that ultimately provides the service; and

- under the current arrangements contracted companies do not have the same level of accountability as the government would if it provided the service direct itself.[354]

As a result, the ALRC recommended that the Victorian government should adopt the provisions of the *Privacy Act* (Cth) and should extend the operation of the regulatory scheme to include service providers contracted with by government agencies.

[However, the ALRC stated that the IPPs in the *Privacy Act* (Cth) are not in an appropriate form to apply to the provision of services such as child care, aged care and disability services. In these cases the ALRC recommended that the IPPs be varied in their application through the development of guidelines outlining how service providers can comply with the principles. The committee has noted in section 6.3 that a code of practice could be developed in relation to the provision of these services.]

The issue of the application of privacy laws to service providers contracted by government agencies is topical at the federal level. The federal Privacy Commissioner has for a number of years recommended that the *Privacy Act* (Cth) be amended to cover the acts and practices of contractors. In May 1997 the federal government announced that it would contract out most of its IT infrastructure and support, and subsequently announced that it would extend the *Privacy Act* (Cth) to apply to all contractors providing services to, or on behalf of, the government which involve the handling of personal information.[355] Legislation to make these changes was introduced into the Commonwealth Parliament on 5 March 1998.[356]

The federal government also announced in February 1998 that the FOI Act (Cth) will apply to requests by individuals for access to, and correction of, personal information about themselves held by contractors on behalf of the government.[357] The Privacy Amendment Bill makes changes to facilitate this and foreshadows another Bill to amend the FOI Act.

---

354 Australian Law Reform Commission, October 1996, op cit, p 5.

355 The operation of the *Privacy Act* (Cth) has already been extended to cover private sector providers of case management for job-seekers and providers of hearing services. See the *Employment Services (Consequential Amendments) Act 1994* (Cth) and the *Hearing Services and AGHS Reform Act 1997* (Cth).

356 Privacy Amendment Bill 1998 (Cth).

357 See the media release dated 3 February 1998 from the office of the federal Attorney-General, Hon Daryl Williams AM QC MP.

8.3.2 Arguments raised in public consultation

Most submissions that addressed this issue agreed that the same privacy obligations which apply to a department or agency out-sourcing the performance of a service should apply to the body contracted to perform the service. However, there were different views on how those privacy obligations should be extended.

The CJC submitted that it could be a matter of contract between the respective bodies, with the contracts referring specifically to the legislative privacy provisions which affect the out-sourcing department or agency.

Others favoured the extension of the privacy legislation. For example, Ms I Graham noted:

> *…bodies performing outsourced services should be regulated by legislation equivalent to that applying to the public sector. Members of the public should not be left dependent on government agencies to prosecute privacy breaches under terms of contracts between the agency and the service provider*.[358]

The ADC-Q submitted that:

> *The awarding of government tenders and contracts could be conditional upon the private sector agency demonstrating it has met relevant guidelines or codes of practice in relation to Information Privacy Principles.*[359]

The Department of Justice stated that out-sourcing is a matter that is best dealt with by the Privacy Commissioner in the development of the guidelines and exemptions in Stage 2 of its proposed privacy regime. The department stated that although no particular view is expressed in its submission, it is likely that outsourcing would be covered by the principles.

8.3.3 Analysis and conclusion

There would appear to be no reason why the same privacy obligations which apply to public sector departments and agencies (either state or local government) should not apply to those bodies which are contracted to perform services that they would traditionally or otherwise perform.

The government's decision to out-source some of its services, whether for cost or other reasons, should not detract from the application of privacy legislation to the handling of personal information which may occur in that process.

The committee agrees with the moves at the federal level to extend the operation of privacy legislation to cover private service-providers contracted with by government departments and agencies and believes such moves should be mirrored in Queensland's privacy regime.

8.3.4 Recommendation

Recommendation 18 - The committee recommends that the Privacy Act (Qld) should apply to private service-providers contracted by Queensland government departments

---

358 I Graham, submission dated 1 August 1997, p 4.

359 Anti-Discrimination Commission Queensland, submission dated 1 August 1997, p 5.

and agencies (either state or local government) to perform services which would otherwise be performed by those departments or agencies.

8.4 THE APPLICATION OF THE PRIVACY ACT (QLD) TO GOVERNMENT OWNED CORPORATIONS

8.4.1 Background

There has been a recent trend for governments to 'corporatise' selected aspects of their business activities. This process involves governments restructuring these selected activities in such a way as to operate on a commercial basis whilst maintaining government ownership. At the state government level in Queensland, the entities so formed are known as Government Owned Corporations[360] (GOCs) and, at the local government level, Local Government Owned Corporations (LGOCs). This corporatisation process is defined and regulated by the *Government Owned Corporation Act 1993* (Qld) (the GOC Act) and the *Local Government Act 1993* (Qld) (the LG Act) respectively.[361] Corporatisation is an important reform initiative in the context of the National Competition Policy.

One of the four key principles of this corporatisation process is 'competitive neutrality' which is defined in s 19 of the GOC Act. The elements of this principle include that, wherever possible, each GOC should compete on equal terms with the private sector and any special advantages or disadvantages the GOC has because of its public ownership or its market power should be removed, minimised or made apparent.[362]

The definition of corporatisation and its key principles are repeated in the LG Act with respect to the reform process for certain 'significant business activities' of local governments.[363] Both the Gold Coast City Council (GCCC) and Logan City Council (LCC) confirmed at the Gold Coast public hearing that local authorities are changing the way they operate and adopting more and more private sector practices.

If an information privacy regime such as that recommended by the committee applies to both the public and private sectors, then obviously GOCs and LGOCs should be caught by that regime. However, if a privacy regime applying only to the state (and local government) public sector is implemented, then determining the application of that regime to GOCs and LGOCs is a more difficult issue.

Some argue that the 'competitive neutrality' principle means that some GOCs and LGOCs, at least in relation to their competitive activities, should not have to comply with a scheme which does not apply to their private sector competitors. Alternatively, it may be argued that privacy laws should only apply to a GOC if it is not in a truly competitive environment (that is, if it represents a monopoly or is a dominant provider) because then there is no competition to provide the equivalent consumer protection.

The *Privacy Act* (Cth) deals with this issue by excluding the application of the IPPs to some public trading enterprises (that is, GOC equivalents) entirely, and by excluding the commercial

360 In other jurisdictions these entities are known as Government Business Enterprises or GBEs.
361 'Corporatisation' is defined in s 16 of the GOC Act and s 458 DE of the LG Act.
362 s 19(d) of the GOC Act.
363 s 458 DE and DF of the LG Act.

activities of a number of others. This is provided for in s 7 of the *Privacy Act* (Cth) and the schedules to the Commonwealth FOI Act.

However, many of the arguments raised in the context of the application of privacy legislation to service providers contracted by government would seem to equally apply in the case of GOCs and LGOCs. This point was made by the ALRC in its submission to DPAC. The ALRC stated that the same concerns with respect to companies contracted by government agencies not being subject to the privacy protection regime arise in relation to the commercial operations of government through the formation of GOC equivalents. (These concerns are noted in the previous section.) Thus, the ALRC recommended in that submission that the application of the provisions of state legislation equivalent to the *Privacy Act* (Cth) should also be extended to the activities of these public enterprise bodies.

Reference to the treatment of GOCs in other areas of administrative law in Queensland is useful, although such treatment does not necessarily represent the model to be followed in relation to privacy legislation.

The FOI Act provides that it does not apply to documents received, or brought into existence, by specified GOCs (such as state electricity entities and the Queensland Investment Corporation) carrying out certain excluded activities.[364] These 'excluded activities' are commercial activities or community service obligations prescribed by regulation.

Similarly, the FOI Act does not apply to documents received or brought into existence, by a LGOC carrying out commercial activities or community service obligations prescribed under a regulation.[365]

The exclusion of GOCs and LGOCs from the FOI Act in so far as their commercial activities are concerned has been examined by the Information Commissioner in his last three annual reports. In particular the Information Commissioner argues two points.

Firstly, the Commissioner considers that GOCs should not be specifically excluded but instead be subjected to the FOI Act and the general exemptions it contains; GOCs' commercial interests would be adequately protected by the exemptions available to agencies generally under the Act. In particular, s 45 of the FOI Act provides that certain matter relating to trade secrets, information of a commercial value and business affairs are exempt from disclosure.

In this regard the Information Commissioner has stated that he agrees with the view expressed by the Commonwealth Ombudsman that all GOCs should be subject to FOI legislation as the question 'goes beyond a test of the operation of the marketplace' (assuming it is competitive).

> *Other considerations (related to Community Service obligations, the public interest, accountability for the exercise of statutory powers and management of public assets) require that the principles of transparency and accountability should apply to GBEs, though they should have the right to claim exemption for commercial and competitive documents under the provision of the Commonwealth FOI Act.*[366]

---

364 See s 11A and schedule 2 of the FOI Act.

365 s 11B of the FOI Act and s 793B of the LG Act.

366 See the Information Commissioner's *Annual Report for 1995/96*, Queensland Government Printer, Brisbane, October 1997, pp 33-34, paras 3.32-3.33.

Secondly, the Information Commissioner argues that excluding GOCs from FOI access is unnecessarily protective and that s 11A in all likelihood extends protection to GOCs beyond that enjoyed by any private sector competitor. This is because s 11A erects a class of documents to which the FOI Act does not apply whether they are in the possession of a GOC or another body such as the Minister, law enforcement or regulatory body.

Accordingly, the Information Commissioner has called for legislative amendments to remove the anomalies caused by s 11A.[367]

In his annual report for 1996/97, the Information Commissioner expresses greater concern with respect to the similar provision which apply to LGOCs and which were introduced during that reporting period. The Information Commissioner states:

> *This amendment is even more disturbing, because it does not appear to require legislative approval for the creation of a LGOC, merely a series of local authority resolutions. It therefore appears possible for a local authority to protect many of its functions from accountability under the FOI Act without the input or overview of Parliament, again in such manner as to put the LGOC in a more protected position, with respect to the application of the FOI Act to documents concerning commercial activities, than any private sector competitor*.[368]

As to the application of other administrative laws to GOCs and LGOCs the committee notes:

- section 18A of the *Judicial Review Act 1991* (Qld) states that that Act does not apply to the decisions of listed GOCs in carrying out commercial activities or community service obligations prescribed by regulation;

- section 793B of the LG Act provides that the *Judicial Review Act 1991* (Qld) does not apply to a decision of a LGOC in carrying out commercial activities or community service obligations prescribed by regulation; and

- section 182 of the GOC Act restricts the power of the Ombudsman to investigate certain GOCs and decisions concerning GOCs (including a decision about a GOC's commercial policy or a statutory GOC in relation to its commercial competitive activities). At the time of the introduction of this provision the Ombudsman expressed concerns regarding the potential for his jurisdiction to be removed from the commercial decisions of agencies as they became statutory GOCs.[369]

8.4.2 Arguments raised in public consultation

There was clear support in the majority of submissions which addressed this issue for information privacy regulation to apply to GOCs.

As the QCCL noted, despite their commitment to the 'level playing field' and to taking on the appearance of being a private corporation, GOCs remain owned by and operate as assets of the government, and as such should be clearly subject to any privacy regime.

---

367 Ibid, pp 34-35, paras 3.34-3.41.

368 Information Commissioner, *Annual Report 1996/97*, Queensland Government Printer, Brisbane, October 1997, p 22, para 3.14.

369 See the Ombudsman's *Annual Report for 1993/94*, Queensland Government Printer, Brisbane, November 1994, p 12.

However, some submissions suggested that the application of a privacy regime to GOCs should depend on whether these entities are operating in a competitive commercial environment. Queensland Rail addressed the issue in some detail and concluded that:

> *…any privacy legislation that applies to GOCs and not the private sector would inhibit their ability to comply with the competitive neutrality principle outlined in the GOC Act. The additional burden imposed would not be shared with the private sector and would disadvantage GOCs through the additional costs associated with compliance.*
>
> *In view of this, QR believes that if privacy legislation is enacted in Queensland in the public sector only, then all GOCs should be exempt from this legislation.*
>
> *However, should it be decided that GOCs should be included, then QR would argue that this should only be to the same extent as GOCs are required to comply with other administrative laws such as the Freedom of Information Act 1992 and the Judicial Review Act 1991. Such a decision would ensure legislative consistency and remove any confusion in the application of the proposed legislation.*[370]

A confidential submission also stated that compliance costs were a factor to be considered in determining whether privacy legislation should apply to some GOCs.

8.4.3 Analysis and conclusion

The above discussion highlights that there are a number of key concerns surrounding the application of administrative law generally to GOCs and LGOCs. The committee believes that this is an area in which further inquiry and consultation should be conducted. Therefore, the committee believes that, at this stage, the Privacy Act (Qld) should apply to the activities of GOCs and LGOCs to the same extent as those entities are subject to the *FOI Act* and *Judicial Review Act*. However, the committee is hesitant to make any firm conclusions and recommendations at this stage regarding the application of proposed privacy legislation to *all* activities of GOCs and LGOCs until further inquiry is undertaken.

Having said this, the committee does recognise that in principle there are clear arguments for the committee's proposed privacy regime to extend to all activities of GOCs and LGOCs. These arguments include the following.

- Protecting the privacy of personal information is good management practice and therefore should be employed by all organisations whether public or private.
- GOCs and LGOCs are still owned and operated by the government and therefore should be subject to the same requirements as public sector agencies.
- The form that a government service provider takes has little effect on its functions and the ability that it has to intrude on the privacy of individuals.

There would appear to be two main arguments against the extension of the Privacy Act (Qld) to the commercial activities of GOCs and LGOCs. Both of these arguments are based on the premise that the application of a privacy regime to this extent would disadvantage the public enterprises in terms of the 'competitive neutrality' principle.

---

[370] Queensland Rail, submission dated 22 July 1997, p 3.

The first argument is that GOCs and LGOCs will be disadvantaged by being subject to a privacy regime as a result of consequent additional compliance costs. However, this argument can be countered on the basis that these organisations, as part of good management practice, should already comply with broad privacy principles such as the IPPs in the *Privacy Act* (Cth). The fact that their private sector competitors might not also employ good management practices is an irrelevant consideration.

The second argument is that GOCs and LGOCs would be disadvantaged if a privacy regime applied to them as they could be forced under the regime to grant access to commercially sensitive information which their private sector competitors would not have to reveal. However, as noted above, the FOI Act to a large extent addresses this concern by providing that certain matter relating to trade secrets, information of a commercial value and business affairs are exempt from disclosure.

The *Privacy Act* (NZ) demonstrates that a similar exception can be built into privacy legislation. Section 28 of that Act provides that an individual's request for access to information can be refused if its non-disclosure is necessary to protect a trade secret or protect information where its disclosure would be likely to unreasonably prejudice the commercial position of the person who supplied, or who is the subject of, the information. (Although, these grounds for refusing access may be outweighed by the public interest in disclosure.)

In order to protect GOCs and LGOCs from being compelled to disclose commercially sensitive information a similar provision could be inserted into the Privacy Act (Qld). Alternatively, the Queensland Privacy Commissioner could issue a code of practice relating to the application of the IPPs to commercially sensitive material of GOCs and LGOCs.

A final argument raised in public submissions was that the application of the Privacy Act (Qld) to GOCs and LGOCs needs to be consistent with the current application of other administrative laws such as the *FOI Act* and the *Judicial Review Act* to those bodies. Again, whilst the committee is taking this position at this stage, this is not on the basis that it believes that there necessarily must be consistency. It might be argued that the importance of good information privacy practices transcends the boundaries of the public sector unlike some of the principles behind other administrative laws which apply purely to government.

8.4.4 Recommendation

Recommendation 19 - The committee recommends that, at this stage, the Privacy Act (Qld) should apply to the activities of GOCs and LGOCs to the same extent as those entities are subject to the *Freedom of Information Act 1992* (Qld) and the *Judicial Review Act 1991* (Qld).

However, the committee does believe that, in principle, the Privacy Act (Qld) should apply to *all* activities of GOCs and LGOCs. The committee recommends that this matter should be part of a larger review of the application of administrative law in general to GOCs and LGOCs.

9. CHAPTER 9 - ENSURING THE EFFECTIVENESS OF THE PRIVACY REGIME

9.1 INTRODUCTION

In order to be effective a privacy regime needs to contain certain features and mechanisms to ensure that: agencies[371] are complying with its terms; it is operating efficiently and effectively; and it is subject to constant review.

The committee has already recommended that its proposed privacy regime contain some features aimed at ensuring its effectiveness. The most significant of these is the establishment of a new officer of the Parliament, namely a Queensland Privacy Commissioner with appropriate functions and powers to oversee the regime.

However, during the course of the committee's research, it discovered a number of other mechanisms which could assist in ensuring the overall effectiveness of the regime. The committee discusses the merit or otherwise of these mechanisms in this chapter.

9.2 PRIVACY OFFICERS

9.2.1 Background, analysis and conclusion

Throughout this report reference has been made to the privacy regime operating in New Zealand. One feature of the New Zealand regime which has not been discussed thus far, is the requirement in s 23 of the *Privacy Act* (NZ) that each agency appoint at least one 'privacy officer'.

Pursuant to s 23, the responsibilities of these officers include:

- the encouragement of compliance by the agency with the IPPs;
- dealing with requests made to the agency pursuant to the Act;
- working with the Privacy Commissioner in relation to investigations conducted pursuant to the Act in relation to the agency; and
- otherwise ensuring compliance by the agency with the provisions of the Act.

The federal Attorney-General's discussion paper of September 1996 regarding privacy protection in the private sector also proposed that privacy officers with similar functions to those listed above be appointed in each organisation. The discussion paper added that:

- it would not be necessary for organisations to appoint a person whose sole function was to be the privacy officer; this officer could undertake functions additional to those placed on them by any privacy legislation; and

[371] 'Agencies' in this sense (and hereafter) refers to state government departments and agencies, local governments, government contractors, GOCs and LGOCs.

- the privacy officer would not be individually liable for any breaches of the IPPs by the organisation.[372]

The committee believes that there would be numerous advantages to the appointment of dedicated privacy officers (charged with functions similar to that in s 23 of the New Zealand *Privacy Act*) in those Queensland agencies covered by the regime. For example, these officers would be able to:

- encourage the agency's compliance with the IPPs and more generally encourage the agency to be more privacy-orientated;
- show a commitment on the part of the agency to privacy;
- assist the Queensland Privacy Commissioner in the performance of his/her functions;
- provide persons dealing with the agency with an identifiable point of contact regarding their privacy queries and concerns;
- build up expertise in dealing with privacy queries which should in turn lead to greater efficiency for the agency and provide its clients with better service; and
- provide an established link between that agency and the offices of the Queensland and federal Privacy Commissioner.[373]

The committee also believes that the costs associated with the appointment of privacy officers would be minimal for two main reasons. Firstly, it would be more cost effective to have an identified person/s dealing with privacy matters than to have them dealt with on an ad hoc basis. Secondly, and as noted by the federal Attorney-General, it would not be necessary for the agency to appoint as a privacy officer a person whose sole functions relate to privacy. The role could be in addition to other functions performed by that officer.

The committee also agrees with the federal Attorney-General's proposal that such officers should not be individually liable for any breaches of the IPPs by the agency.

9.2.2 Recommendation

Recommendation 20 - The committee recommends that the Privacy Act (Qld) place an onus on each department and agency covered by the Act to ensure that there is within that organisation an individual whose responsibilities include:

- **encouraging compliance by the organisation with the IPPs;**
- **dealing with requests made to the organisation pursuant to the Act;**
- **working with the Queensland Privacy Commissioner in relation to certain investigations conducted pursuant to the Act in relation to the organisation; and**
- **otherwise ensuring compliance by the organisation with the provisions of the Act.**

372 Federal Attorney-General, 1996, op cit, p 24.
373 Ibid.

The committee recommends that the Privacy Act (Qld) provide that such officers are not to be individually liable for any breaches of the IPPs or the Act in general by the department or agency.

9.3 ANNUAL REPORTING REGARDING PRIVACY BY AGENCIES AND THE QUEENSLAND PRIVACY COMMISSIONER

9.3.1 Annual reporting by agencies

9.3.1.1 Background, analysis and conclusion

It was noted in chapter 8 that the Redland Shire Council in its submission to the committee suggested that local governments could be required under their legislation to report on privacy issues in their annual reports. This, it was submitted, would further emphasise the importance of promoting the protection of privacy in local government, and serve as a monitoring mechanism by insisting that local governments are aware of the necessity to protect information in their possession.

The committee believes that whilst this suggestion was raised in the context of local governments, it is a suggestion which could equally apply to all agencies covered by the proposed legislation.

It is important that the implementation of IPPs is not merely, or seen to be merely, a token gesture by agencies. Placing a responsibility on agencies to regularly report with respect to matters such as their compliance with the IPPs and the privacy regime generally should encourage compliance and serve as an additional monitoring mechanism.

In addition, these reports should assure clients of those agencies as to the privacy measures that they have in place. As noted at the very outset of this report, clients must have confidence in the data technology which is increasingly being employed by departments and agencies if they are to be expected to use and trust it.

Therefore, the issue arises as to what 'privacy' information should be reported by agencies and how and where this information should be reported.

In chapter 6 the committee recommends that the Privacy Act (Qld) contain IPPs modelled on those currently contained in s 14 of the *Privacy Act* (Cth). IPP 5 of those Commonwealth principles require that a record-keeper shall maintain a record setting out a number of matters including:

- the nature of the records of personal information kept by or on behalf of the record-keeper;
- the purpose for which each type of record is kept;
- the classes of individuals about whom records are kept;
- the period for which each type of record is kept;
- the persons who are entitled to have access to personal information contained in the

records and the conditions under which they are entitled to have that access; and

- the steps that should be taken by persons wishing to obtain access to that information.

Pursuant to clause 4 of IPP 5 the record-keeper is obliged to give the Privacy Commissioner a copy of this record in June each year.

The object of this requirement would appear to be to assist citizens in establishing and enforcing their privacy rights under the legislation. In this regard it is similar to the requirement already placed on agencies by s 18 of the FOI Act (Qld). Section 18 requires agencies to publish annually an up-to-date statement of affairs of the agency. This statement must contain matters such as a description of:

- the agency's structure and functions;
- the various kinds of documents that are usually held by the agency including those that are available for inspection at the agency; and
- the arrangements that exist to enable a member of the community to obtain access to the agency's documents and to seek amendment of the agency's documents concerning the person's personal affairs.

Therefore, to some extent there is already an annual reporting requirement on agencies in the privacy regime proposed by the committee pursuant to IPP 5. As it currently stands, this annual 'report' will be to the Queensland Privacy Commissioner.[374] However, for the reasons suggested by the Redland Shire Council, the committee believes that in addition to publishing this record, other privacy matters should be addressed as part of an agency's annual report.

As has already been noted in section 7.5 of this report, in Canada the federal *Privacy Act* requires the head of every government institution to prepare for submission to Parliament an annual report on the administration of the *Privacy Act* within the institution during each financial year. Every report once tabled is then referred to a parliamentary committee.

In Queensland the *Financial Administration and Audit Act 1977* (Qld) provides that departments and statutory authorities are to annually prepare a report which must include a report on the operations of the entity during the financial year and such information as the appropriate Minister directs to enable him/her to assess the efficiency, effectiveness and economy of the entity.[375]

Thus, the committee envisages that many departments will address privacy issues in their annual reports as part of reporting on their operations, efficiency and effectiveness. The committee also believes that the Queensland Privacy Commissioner should, as part of his/her functions, assist agencies in this regard by publishing generic guidelines as to the types of privacy matters that their annual reports should address. These guidelines should give agencies the flexibility to deal with topical information and non-information privacy issues such as data-matching, smart cards, video surveillance etc as they arise during the year.

---

[374] The committee has previously recommended in section 6.1 of this report that the Queensland Privacy Commissioner should have a *discretion* as to whether to publish a consolidation of these records provided by agencies.

[375] See s 37B in relation to the requirement that departments prepare annual reports and s 46J in relation to the requirement that statutory bodies prepare annual reports.

9.3.1.2 Recommendation

Recommendation 21 - The committee confirms that departments and agencies covered by the Privacy Act (Qld) should be required to provide annually to the Queensland Privacy Commissioner a copy of the record maintained in accordance with the Queensland equivalent of IPP 5 of the *Privacy Act 1988* (Cth).

In addition, the committee recommends that departments and agencies should report on privacy issues that affect them in their annual reports. The Queensland Privacy Commissioner should issue generic guidelines as to the type of privacy matters that should be canvassed in annual reports.

9.3.2 Annual reporting by the Queensland Privacy Commissioner

9.3.2.1 Background, analysis and conclusion

Clearly the Queensland Privacy Commissioner should be required to report annually regarding his/her operations.

Section 97 of the *Privacy Act* (Cth) requires the federal Privacy Commissioner to, as soon as practicable after 30 June in each year, give to the Minister a report which includes:

- an assessment of the operation of the Act during the year; and
- a statement on the performance of the Commissioner's function under s 27(1)(n) of the Act (that is, to encourage corporations to develop programs for the handling of records of personal information that are consistent with the OECD Guidelines).

The Minister is then required to table that report in the House of Representatives within 15 sitting days of receiving that report.

Section 24 of the *Privacy Act* (NZ) also provides that the New Zealand Privacy Commissioner is to report each year to the responsible Minister regarding the operation of that Act during the year.[376]

The committee believes that the Queensland Privacy Commissioner should be similarly required to report annually in relation to the operation of the *Privacy Act* and the exercise of his/her functions generally. More specifically this report should include details on:

- the number and nature of complaints made against agencies (without breaching the confidentiality of the complainants and the outcome of those complaints;
- any recommendations that the Queensland Privacy Commissioner has made with respect to agencies;
- the operations of the privacy advisory committee during the year;
- the manner in which privacy concerns emerging as a result of new technology are

[376] The only limit on this provision is that s 120 of the New Zealand Act provides that the Commissioner shall not make any comment that is adverse to any person unless that person has been given an opportunity to be heard.

being, or should be, addressed; and

- any other matters affecting agencies covered by the regime and privacy.

As the Queensland Privacy Commissioner is to be an officer of the Parliament, this annual report should be to Parliament. In this regard the committee notes s 26 of the *Parliamentary Commissioner Act 1974* (Qld). It provides that the Ombudsman shall as soon as practicable after 30 June each year, cause to be laid before the Legislative Assembly a report on the exercise of the Commissioner's functions during the 12 months (or in the case of the first report, the lesser period) ending on that date.

Of course, this annual reporting requirement should be in addition to the other reporting powers that the committee has already recommended for the Queensland Privacy Commissioner.

9.3.2.2 Recommendation

Recommendation 22 - The committee recommends that the Privacy Act (Qld) contain a provision requiring the Queensland Privacy Commissioner to report annually to Parliament with respect to the exercise of his/her functions and the operation of the Privacy Act (Qld).

9.4 STRATEGIC REVIEWS OF THE QUEENSLAND PRIVACY COMMISSIONER

9.4.1 Background, analysis and conclusion

It will be recalled that in section 7.5 of this report the committee recommended that the Queensland Privacy Commissioner should be an independent officer of the Queensland Parliament, like the Auditor-General and the Ombudsman, and that as part of this independence the Legal, Constitutional and Administrative Review Committee (LCARC) should have a number of functions in relation to the Queensland Privacy Commissioner. These functions mirror the functions that the committee currently has in relation to its involvement in the termination, suspension and removal of the Ombudsman and in the formulation of that officer's budget.

However, a final matter which the committee has yet to consider is whether the current requirement in s 32 of the *Parliamentary Commissioner Act 1974* (Qld) in relation the conduct of 'strategic reviews' of the Ombudsman should also apply to the Queensland Privacy Commissioner. [A similar requirement in relation to the conduct of strategic reviews of the Queensland Audit Office (QAO) appears in s 72 of the *Financial Administration and Audit Act 1977* (Qld).]

Whilst the term 'strategic review' is not defined in either of the relevant statutes, these reviews are basically five-yearly reviews of the performance, management and structure of these offices. This conclusion can be drawn from:

- a study of those portions of EARC's *Report on Review of Public Sector Auditing in*

Queensland[377] as a result of which the requirements in relation to the conduct of strategic reviews were inserted in relation to the QAO and subsequently the Ombudsman[378];

- the report on the inaugural strategic review of the QAO[379]; and
- the terms of reference for the inaugural strategic review of the Ombudsman which is currently being conducted.

Strategic reviews are conducted by an appropriately qualified person appointed by the Governor in Council after the Minister has consulted with the Ombudsman and Auditor General about their appointment and the terms of reference for the review.

The committee believes that the conduct of regular reviews, by an external consultant, can be most valuable in assessing the performance and operational efficiency of an office. Therefore, the committee believes that the requirement to conduct strategic reviews should be extended to the Queensland Privacy Commissioner.

Moreover, because the committee proposes that the Queensland Privacy Commissioner be an officer of the Parliament, the committee believes that the LCARC should have certain responsibilities in relation to the conduct of these reviews. For consistency, the provision in relation to strategic reviews of the Queensland Privacy Commissioner should be modelled on s 32 of the *Parliamentary Commissioner Act 1974* (Qld). However, as the inaugural strategic review of the Ombudsman's office is being conducted at the time of writing this report, the committee flags that it may later recommend amendments to that section as a result of that review. For consistency the committee would expect that any recommended amendments that it may have to s 32 would also be incorporated in the corresponding section in the Privacy Act (Qld).

9.4.2 Recommendation

Recommendation 23 - The committee recommends that strategic reviews of the Office of the Queensland Privacy Commissioner be conducted at regular intervals and that in this regard a provision modelled on s 32 of the *Parliamentary Commissioner Act 1974* (Qld) should be inserted into the Privacy Act (Qld).

The committee makes this recommendation subject to any changes that it may propose to s 32 in response to the inaugural strategic review of the Ombudsman's office which is currently being conducted.

---

377 EARC, Government Printer, Brisbane, 1991, pp 181-183. EARC's parliamentary committee, PCEAR, subsequently endorsed EARC's recommendation in relation to what it called 'performance audits' with one slight amendment so that the performance auditor is appointed by the Governor in Council (as opposed to the Parliamentary Service Commission) after consultation with the Public Accounts Committee. PCEAR, *Public Sector Auditing*, Queensland Government Printer, Brisbane, 1991.

378 Whilst EARC's recommendations in its 1991 report related to strategic reviews of the QAO, a similar requirement was inserted into the *Parliamentary Commissioner Act 1974* (Qld) by virtue of the *Parliamentary Committees Act 1995* (Qld). This amendment provided for strategic reviews of the Ombudsman to also be conducted.

379 T A Sheridan, *Report of the strategic review of the Queensland Audit Office*, Government Printer, Brisbane, 19 July 1997. See particularly the terms of reference of that review at p 21.

9.5 OFFENCE PROVISIONS

9.5.1 Background, analysis and conclusion

A final consideration with respect to ensuring the effectiveness of the proposed privacy regime is the need for compliance mechanisms in the form of offence provisions.

The *Privacy Act* (Cth) provides that it is an offence for a person, without reasonable excuse, to:

- refuse or fail to attend before the Commissioner;
- refuse or fail to be sworn or make an affirmation;
- wilfully obstruct, hinder or resist the Commissioner in the performance of his/her functions under the Act;
- refuse or fail to give information when required under the Act; or
- refuse or fail to answer a question or produce a document or record when required under the Act.[380]

It is also an offence for a person to furnish information or make a statement to the Commissioner knowing that it is false or misleading in a material particular.[381]

The penalty for an individual in relation to all of the above offences is $2 000 or imprisonment for 12 months or both.[382]

In the case of the *Privacy Act* (NZ) the following persons commit an offence:

- any person who, without reasonable excuse, obstructs the Commissioner, or refuses or fails to comply with an order of the Commissioner; or
- any person who makes a statement or gives any information to the Commissioner knowing that it was false or misleading, or misrepresents any authority held under the Act.[383]

Section 127 also provides that such persons are on summary conviction liable to a fine of up to $2 000.

The Department of Justice recommended that its proposed Privacy Commissioner Bill should contain three offences (with a maximum penalty of 10 penalty units which is currently $750.00) and that proceedings for these may be disposed of summarily by a magistrate sitting alone. These offences are:

- *without lawful excuse to hinder or obstruct the Commissioner in an investigation*

380 ss 65-66.

381 s 65(3).

382 See ss 65-66. In the case of refusing or failing to give information or answer a question or produce a document or record, a body corporate can be subject to a fine of $10 000. See s 66(1).

383 s 127.

- *without lawful excuse to refuse to comply with a lawful requirement of the Commissioner*

- *to make false or misleading statements.*[384]

In chapter 7 of this report the committee recommended that the Queensland Privacy Commissioner should have powers modelled on those granted to the federal Privacy Commissioner by the *Privacy Act* (Cth). Therefore, logically the Privacy Act (Qld) should include substantially the same offence provisions as contained in the Commonwealth Act. In this regard the committee notes that that the offences suggested by the Department of Justice are in fact included in the offences under the *Privacy Act* (Cth), although the penalties are substantially less.

The committee believes that a penalty must be high enough so that it has a deterrent effect. In the case of a privacy regime, the higher sum of $2 000 would appear more appropriate.

9.5.2 Recommendation

Recommendation 24 - The committee recommends that the Privacy Act (Qld) contain offence provisions modelled on the offence provisions contained in the *Privacy Act 1988* (Cth).

[384] Department of Justice, submission dated July 1997, p (ix).

PART 3

10. CHAPTER 10 - PRIVACY IN THE PRIVATE SECTOR

10.1 PRIVACY IN THE PRIVATE SECTOR

10.1.1 Background

Thus far the committee's report has concentrated on protecting the privacy of information about individuals held by Queensland government departments and agencies, its contractors and GOCs. In this Part of the report the committee canvasses:

- whether there also needs to be additional regulation to that which currently exists regarding the privacy protection afforded to information about individuals in the private sector; and
- if so, what form that regulation should take.

The committee noted at the very outset of this report that the rapid development of technology, particularly information technology, means that it is now easier for persons and organisations to collect and use information concerning individuals. This observation relates equally to the private sector as it does to the public sector.

It was also noted in chapter 3 of this report that there are currently few measures regulating information privacy in the private sector in Australia. This regulation is confined to some redress available under the common law and the limited coverage of the private sector by the *Privacy Act* (Cth). There have also been some ad hoc self-regulatory attempts to address information privacy via industry codes of conduct. Therefore, it is argued by many that existing laws and guidelines do not adequately protect the privacy of individuals when it comes to the collection and use of information about them in the private sector.

However, whilst this may on the face of it indicate that the privacy legislation proposed by the committee to apply to information held by the government should also apply to information held in the private sector, there are a number of other important considerations which must be taken into account. These considerations include:

- arguments for and against further regulation of information privacy in the private sector;
- the form that any further regulation should take;
- the requirements and effect of the 1995 European Union *Directive on the protection of individuals with regard to the processing of personal data and on free movement of such data* (the EU Directive)[385] on the above;
- current developments at the Commonwealth level in this area; and

[385] Refer to chapter 2 for a brief introductory comment on this directive.

- the need for national consistency in standards required of the private sector.

Arguments for and against further regulation of information privacy in the private sector

Arguments commonly raised as to why current information privacy protection in the private sector is adequate and further regulation should not be introduced include the following.

- Different information privacy regimes should apply to the two sectors on the basis that persons are compulsorily required to provide information to governments whereas much of the information collected by the private sector is not required compulsorily.

- 'Market forces' will provide an adequate level of privacy protection as good business dictates that adequate protection must be given to information held about both customers and employees. If an organisation does not give due regard to privacy then they will lose business to their competitors.

- The compliance costs associated with any further regulation will be too high. These costs could include costs associated with: amending forms used in organisations; changing the manner in which information is collected; granting persons access to their information; and costs associated with training staff.[386]

Conversely, arguments for further regulation than that which currently exists include the following.

- The privacy afforded to personal information is a real concern to the community as highlighted by surveys such as that conducted the federal Privacy Commissioner in 1995.[387] These concerns are not restricted to the privacy of information held by governments. Additional mechanisms should be introduced to address these concerns. Many other overseas jurisdictions have recognised this and passed privacy legislation applying to their public and private sectors.[388]

- Many private sector organisations themselves recognise the importance of information privacy and support further information privacy regulation. Seventy percent of respondents to a nationwide survey conducted by Price Waterhouse in 1997[389] supported the introduction of privacy legislation to cover the corporate sector. As noted in the report on that survey:

> *This is in contrast to the Government view that legislation would add unnecessary burden and overhead to Australian business. Of the organisations surveyed, it was found that 79% felt only minor changes would be required to their business practices in order to comply with legislation, highlighting the fact that Australian business does not believe that there will be significant costs associated with applying good privacy practice.*[390]

386 For a general discussion regarding these arguments see the federal Privacy Commissioner's August 1997 consultation paper, op cit, pp 4-8.

387 Federal Privacy Commissioner, *Community Attitudes to Privacy*, op cit.

388 These jurisdictions include New Zealand, Hong Kong, the Canadian province of Quebec and most European jurisdictions. Refer to chapter 4 of this report for further discussion in this regard.

389 Price Waterhouse, *Privacy Survey 1997*, Melbourne, 1997.

390 Ibid, p 3. The reference to the 'government' here is to the federal government.

- In order to maximise the economic and social benefits of the 'information economy' of which Australia is now a part, consumers must have confidence in the technology which is an essential component of that economy. Regulation designed to ensure the protection of information privacy will help to assure consumers that this new technology will not allow their personal information to be misused. This will, in turn, encourage consumers to utilise this new technology.

- In the absence of further 'across the board' regulation there is no incentive for responsible businesses to introduce privacy policies if maverick competitors can continue to misuse personal information with impunity. A related argument is that without further regulation there is no way to deal with 'free riders'. The federal Privacy Commissioner describes 'free riders' as organisations that, in the context of a voluntary privacy scheme, choose not to commit themselves to either the standards or mechanisms, but which gain a benefit from the public perception that a scheme is in place.[391]

- Without adequate information privacy regulation trade and hence economic wealth and jobs will be at stake.[392] In particular, mention has already been made of the 1995 EU Directive. In her August 1997 consultation paper the federal Privacy Commissioner quoted the following statement from a recent US government paper:

> *No discussion of [on-line] privacy can be complete without appropriate consideration of the EU Directive and its implications for international trade in the Information Age.*[393]

This last point regarding the EU Directive requires further consideration.

The EU Directive makes it mandatory for the fifteen European Union member countries to have in place consistent and comprehensive information privacy laws by October 1998.[394] The Directive further makes it mandatory for those member countries (also from October 1998) to prohibit the transfer of personal data to any country that does not have 'an adequate level of protection' with respect to the processing of personal information.[395] (These are called 'data export prohibitions'.)

Whilst the term 'adequate level of protection' is defined in the Directive[396], some commentators have stated that it is unclear what exactly what will constitute adequacy.[397]

The EU Directive also provides a number of exceptions to the 'adequate protection' requirement.

Firstly, member states can provide that transfers to third countries which do not ensure an adequate level of protection may take place if one of six conditions are satisfied. These

---

391 Federal Privacy Commissioner, August 1997, op cit, p 17, para 76.

392 S Woolley, 'Should we legislate for privacy?', *The Australian*, 5 March 1998, p 11.

393 Federal Privacy Commissioner, August 1997, op cit, p 7.

394 For further details as to the European Directive see G Greenleaf, 'The European Privacy Directive - Completed', *Privacy Law and Policy Reporter*, vol 2, no 5, June/July 1995 and G Greenleaf, 'European Privacy Directive and Data Exports', *Privacy Law and Policy Reporter*, vol 2, no 6, August 1995.

395 See article 25(1).

396 See article 26(2).

397 See G Greenleaf, paper presented to the 1997 Australian Privacy Summit, 'The European Union's privacy directive - New orientations on its implications for Australia', Sydney 21-22 October 1997, pp 11-14.

conditions include the unambiguous consent of the data subject or where the transfer is necessary for the performance of a contract, on important public interest grounds or to protect the vital interests of the data subject.[398]

Secondly, member states can authorise a transfer of personal data to a third country which does not ensure an adequate level of protection where the data controller adduces 'adequate safeguards' with respect to the protection of a person's privacy. In particular this 'adequate safeguards' exception seems to relate to safeguards resulting from appropriate contractual clauses.[399]

However, in both of the above cases these exceptions cannot be relied upon until they are embodied in the national legislation of the member states. Further, whilst the first category of exceptions are mandatory, member states have a discretion as to whether to recognise the 'adequate safeguards' exception.[400]

In addition to the European countries, certain Asian countries are also introducing privacy laws which contains data export prohibitions. These countries include Hong Kong and Taiwan.[401] Malaysia will reportedly also be introducing similar legislation in the short term.[402]

What form should any further regulation take?

If privacy protection of information held in the private sector is to extend beyond the ad hoc self-regulation which currently exists, then there must be consideration given to what form this regulation should take.

The two primary means of regulation would appear to be:

- a more structured self-regulatory framework consisting of standard principles which are adopted in industry codes but in relation to which compliance is encouraged perhaps by a scheme administrator; or
- a legislative scheme.

Arguments in favour of self-regulation by way of industry codes include:

- flexibility, in that codes are able to meet the specific needs of particular industries and/or specific types of activities that are performed across a number of industries;
- the ability for codes to be constantly updated as new technology is introduced into the industry;
- greater industry involvement and consultation in the development of codes which should lead to their greater acceptance; and

398 These are contained in the proviso to article 26(1). For further discussion on these conditions see Greenleaf, 1997, ibid, pp 16-18. Greenleaf notes that these exceptions are not as broad as they first appear.

399 This proviso is contained in article 26(2).

400 Greenleaf, 1997, op cit, p 18. Greenleaf also notes that the only implementing laws at the date of his paper (that is, the laws of Greece) do not recognise any contractual or other forms of 'adequate safeguards'.

401 Greenleaf, ibid, p 6.

402 Woolley, op cit.

- cost, as arguably industry codes are cheaper because they result in a reduction of 'red tape'. (Although others argue that the costs of self-regulation are in fact higher than those applicable under a legislative scheme as self-regulation means that compliance costs are borne by the bodies participating in the scheme whereas under a legislative scheme these costs are largely borne by the state administrator of the scheme, such as a privacy commissioner.[403])

The primary arguments against self-regulation include lack of consistency, lack of certainty in standards and, notably, lack of enforceability. In a paper presented to the committee's seminar on privacy, Professor Bill Caelli argued that government intervention and legislation are both needed to set the necessary levels of security and safety in the information technology used to provide the information services that form the national and global information infrastructure.

> *I know of no case where appropriate levels of security have ever been introduced by the private sector into any industry on a totally voluntary basis without the 'big stick' of Government legislation—legislation aimed at protecting the public. Industry codes or the much vaunted 'self-regulation' works for minimal changes to accepted industry practice—a sort of control over errant companies who stray but within certain bounds. Those innocent citizens affected by the actions of a wildly errant company have little recourse in such schemes. That is where the law of a nation comes in; indeed isn't it the very base for the rule of law?*
>
> *For privacy protection, the self-regulation model will simply NOT work.*[404]

Recent developments

As noted in chapter 4 of this report, there have been a number of recent developments in Australia regarding the issue of regulating information privacy in the private sector. In the course of these developments the arguments for national consistency in standards required of the private sector have become evident.

These recent developments were initiated in September 1996 when the federal Attorney-General released a discussion paper outlining a possible co-regulatory approach to extend privacy protection to the private sector. This approach, which drew heavily on the New Zealand model, involved a general set of statutory IPPs together with provision for the development of suitable codes of practice modifying the application of the IPPs to suit specified information, activities, organisations, industries or professions.

The suggestion was that this proposed privacy regime would extend to all individuals and private sector organisations (including all activities of government business enterprises) to the extent permitted by the Commonwealth Constitution. There would also be certain restrictions placed on the transfer of personal information out of Australia.

On the basis of this proposal, state privacy legislation covering the private sector would not have been necessary.

However, in March 1997 the Prime Minister announced that the Commonwealth would not be implementing privacy legislation for the private sector. The Prime Minister's reasoning behind

---

403 See, for example, Greenleaf, 1997, op cit, p 22.

404 Paper presented to the committee's privacy seminar, Brisbane, 17 November 1997, p 3.

this decision was the need to reduce regulatory burdens so as not to further increase compliance costs for business.

The Prime Minister also asked the state Premiers and Chief Ministers not to introduce privacy legislation covering the private sector within their respective jurisdictions. Both the Queensland Premier and the Northern Territory Chief Minister agreed to this request.

As an alternative, the Prime Minister offered the services of the federal Privacy Commissioner to assist business in the development of voluntary codes of conduct to meet privacy standards.[405]

As a result of the Prime Minister's announcement, in August 1997 the federal Privacy Commissioner released a consultation paper *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector*. This paper puts forward a scheme for discussion consisting of three components:

- principles or standards for the handling of personal information;
- processes for business to 'sign on' to the scheme, and for promoting and monitoring compliance with the principles; and
- mechanisms for handling complaints about breaches of the principles, and providing effective remedies for people affected.

The scheme also clearly recognises the calls for national consistency in privacy standards across all industries in Australia. As the Commissioner notes in the paper, different state and territory laws would create an administrative nightmare for private sector organisations which are trying to operate nationally and internationally. This was also made clear in submissions to the federal Attorney-General's 1996 discussion paper.

National consistency also has the support of the federal and, apparently, the Victorian governments. As noted in chapter 4 of this report, indications are that Victoria may enshrine the national principles emerging from the Commissioner's process in its proposed privacy legislation.[406] This would facilitate meeting the objective of national privacy standards at least so far as the private sector is concerned.

The need for national consistency has also been recognised at the federal level through the establishment of the 'Online Council' to promote and facilitate electronic communication and electronic service delivery. The Council comprises state and territory ministers and local governments representatives who meet twice a year to discuss policy issues relevant to the information economy. At its meeting held in September 1997, the Online Council recognised the desirability of a national approach to privacy and agreed to the formation of an Online Council working party to work with the federal Privacy Commissioner to develop the underlying principles of a data protection regime for the online economy.[407]

The issue of privacy has also been on the agenda of the Standing Committee of Attorneys-General (SCAG) for some time. In January 1996 a SCAG Privacy Officers Working Group

---

405 See the Prime Minister's media release concerning privacy legislation dated 21 March 1997.

406 See also the comments by the federal Privacy Commissioner regarding other state and territory initiatives in her August 1997 consultation paper, op cit, p 13.

407 See media release 'Governments agree on online priorities', 12 September 1997.

was established and apparently this group has facilitated the exchange of information on privacy law reform developments between members of SCAG.[408]

Subsequent to the release of the August 1997 paper, the Commissioner engaged in wide consultation in which she sought views from business, consumer, privacy advocacy and government representatives as to the scheme proposed in that paper.

In November 1997 the Commissioner made a number of observations flowing from that consultation process.[409]

- There is a concern that a patchwork of industry or sector-specific privacy codes will result from the various federal and state privacy initiatives currently underway.

- If a national set of privacy principles is to be agreed upon it must occur within the next two or three months otherwise one of the above initiatives will proceed with its own set of principles.

- There is clearly a call for one set of national privacy principles (as opposed to a patchwork), however, it is recognised that these principles may have to be modified to cater for some particular industries or sectors such as health.

- A national approach is essential in order to provide an adequate framework for the fast growing international electronic commerce sector which will have a significant impact on all Australian business.

As a result, the Commissioner decided to separate the private sector consultation process into two components; firstly, the development of a national set of information privacy principles for the private sector and secondly, the establishment of compliance mechanisms. Given the desirability for national principles to be agreed upon before one of the state or federal initiatives came up with its own set of principles, the Commissioner set this first task as a high priority.

Thus, in February 1998 the federal Attorney-General and the Commissioner launched the *National principles for the fair handling of personal information* (the 'national principles'). According to the Commissioner, the aim in developing these principles was to 'devise a benchmark which is relevant and flexible in the business context without compromising core privacy standards'.[410] The Commissioner also noted that it was important that these principles meet international best practice given overseas developments particularly in Europe.

The Commissioner is now addressing implementation issues associated with that proposed scheme.

During the course of the Commissioner's process there have been a number of other developments with respect to privacy protection in the private sector.

- In April 1997 the 'Wallis Inquiry', which was established by the Federal Treasurer, tabled its final report in relation to its Financial Services Inquiry. In that report the inquiry made a number of observations and recommendations concerning privacy,

408 Refer to the Department of Justice's submission to the committee, 29 July 1997, p 35.

409 These observations were embodied in a letter dated 21 November 1997 from the federal Privacy Commissioner to identified stakeholders and bodies interested in the consultation process.

410 Refer to the Commissioner's foreword to those principles, op cit, p 3.

particularly if a privacy regime is to extend to the financial services sector. It was noted that any extensions to privacy laws should apply only at a national level as uncoordinated action at the state and territory level could result in considerable additional costs and inefficiencies.[411]

- As already noted, in April 1997 the federal government announced that it would outsource its information technology activity and accordingly it would amend the *Privacy Act 1988* (Cth) to apply to contractors handling personal information on behalf of the government. This was later extended to apply to all contractors and not just those involved in information technology outsourcing. It has also been noted that this amending legislation, the Privacy Amendment Bill 1998, was recently introduced.

- On 1 July 1997 the new *Telecommunications Act 1997* (Cth) became operative. This Act allows bodies and associations that represent sections of the telecommunications industry to develop voluntary industry codes of practice regarding a range of issues including privacy.[412] However, there is also provision for, and an expectation that, the Australian Communications Authority will register many of the codes making them legally-binding standards. Privacy concerns about this legislation and the fact that the privacy regime applicable to the telecommunications sector may differ to other sectors have been expressed.[413]

- In September 1997 Senator Stott Despoja of the Australian Democrats introduced a Private Member's Bill into the Commonwealth Parliament which attempts to extend the *Privacy Act* to cover the private sector, expand the IPPs, and allow the Privacy Commissioner to issue codes of practice modifying the operation of the IPPs in relation to particular industries, professions or callings.[414] The Bill proposes that these codes of practice will commence when a resolution approving the code is passed by each House of the Parliament.[415]

Thus, there remains some debate as to whether there should be a regulatory or legislative scheme governing information privacy in the private sector. Many consumer and advocacy groups have boycotted the Commissioner's consultation process as a sign of protest to a regime that may involve anything other than legislation.[416]

There is also still much debate as to whether a voluntary self-regulatory scheme will satisfy the EU Directive.

Until recently, guidance as to how the EU Directive would be interpreted and administered was scant. However, now developments including publications by the EU's *Working Party on*

411 S Wallis, *Financial System Inquiry: Final Report*, Australian Government Printing Service, Canberra, March 1997, pp 517-524 and in particular p 523.

412 See s 113 of the Act which sets out examples of matters that may be dealt with by industry codes and standards. Section 113(3)(f) refers to privacy matters.

413 See for example N Stott Despoja, 'Personal and Private', *Alternative Law Journal*, vol 22, no 4, August 1997 and comments the federal Privacy Commissioner in her *Ninth Annual Report*, op cit, pp 46-48.

414 The Privacy Amendment Bill 1997 was introduced by Senator Stott Despoja on 25 September 1997.

415 Clause 11 of the bill deals with codes of practice.

416 See J Hilvert, 'Voluntary privacy code rejected', *The Australian*, 2 September 1997, p 39.

the Protection of Individuals with Regard to the Processing of Personal Data have shed some light on what impact the EU Directive may have on Australia.[417]

In a recent paper[418] Greenleaf canvasses in detail these developments, the implications of the EU Directive for Australia and what might constitute 'an adequate level of protection' and 'adequate safeguards' as required by the EU Directive before data can be exported.

Greenleaf concludes that the only certain way for Australia to be readily included in the 'white list' of countries with 'adequate protection' is for it to pass privacy legislation covering six core EU Directive principles and to support them with enforcement mechanisms. He adds that the scheme proposed in the Attorney-General's 1996 discussion paper may have satisfied the necessary requirements.

Greenleaf further notes that alternative approaches are likely to result in considerable difficulties for companies wishing to obtain personal information from Europe. In this regard he notes:

- voluntary codes of conduct and technical standards with nothing more would be unlikely to be 'adequate protection' although they could be if supported by legislation. In addition to 'best practice' privacy principles, 'adequacy' requires features such as 'independent supervision, serious sanctions and a high level of proven compliance';

- the mandatory exceptions to 'adequate protection' are limited in that they depend on national legislative implementation in fifteen countries; and

- attempts to provide 'adequate safeguards' via contractual terms are also dependent on implementation in national legislation.[419]

Whilst other commentators share concerns as to Australia's likelihood of being 'white-listed' and warn that unless privacy legislation is introduced local companies could be forced to move their electronic commerce offshore, [420] not all agree.

The federal Attorney-General in a speech made in May 1997, stressed that the protective mechanism required by the EU Directive is an 'adequate' rather than 'equivalent' level of protection, and that even where a non-European Union country does not ensure an 'adequate level of protection', the EU Directive still permits transfers in a number of circumstances.[421]

Most recently it has been reported that the federal Opposition will use the Privacy Amendment Bill 1998 to push for full legislative coverage of information privacy in the private sector.[422]

---

417 See for example the Working Party's *First Orientations of Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*, 26 June 1997, European Commission, Directorate General XV, XV D /5020/97-EN final and also the *Working Document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?*, 14 January 1998, European Commission, Directorate General XV, DG XV D /5057/97 final (WP 7).

418 Greenleaf, 1997, op cit.

419 Ibid, p 21.

420 See the comments of Peter McNally reported in an article by T McIntosh, 'Privacy vital to business', *The Australian*, 15 April 1997, p 44.

421 Speech given by the Attorney-General to the Banking Law & Practice Conference, Sydney, 22 May 1997.

422 H van Leeuwen, 'Opposition presses for broadening of planned privacy law', *Australian Financial Review*, 31 March 1998.

10.1.2 Arguments raised in public consultation

Overall, submissions clearly indicated that privacy regulation additional to that which currently exists should apply to the private sector.

Many submissions received from government departments and agencies and advocacy, consumer and other groups argued that this additional regulation should be via legislation.

Arguments raised in this context included:

- the current trend towards outsourcing, corporatising and privatising government functions means that privacy legislation which only covers the public sector is ineffective and the extension of privacy legislation to these contractors, GOCs and privatised bodies is important as many will be given a considerable amount of personal information;

- there is a need to regulate the use and sale of certain data by private sector organisations such as data lists for use in tele-marketing and direct marketing, and the operation of tenancy databases by private companies;

- further privacy protection of the private sector is needed to comply with international privacy standards and failure to do so may adversely affect trade; and

- a large component of the private sector is comfortable about further privacy regulation being applied to their operations.

Although, the Department of Justice recommended that:

> *… at this time, privacy regulation should only apply to the public sector and not to the private sector. However, that Queensland be supportive of the role that the Commonwealth Office of the Privacy Commissioner is playing in assisting business in the development of voluntary codes of conduct and in the meeting of privacy standards, if necessary, on an international level*.[423]

Submissions received from private sector organisations varied in their response as to whether regulation beyond current self-regulation was required, although there was a clear statement that if any scheme is to be introduced then it must be done on a consistent national rather than state-by-state basis. As noted by American Express:

> *It is the fundamental belief of American Express that for legislation to be truly effective it needs to be national and uniform. State-based legislation, while addressing local needs, adds unnecessary compliance costs for trans-border commerce*.[424]

The Australian Bankers' Association also submitted:

> *There is one overriding factor in implementing a private sector information privacy protection regime in Australia; that is, the regime must be* ***a single, nationally***

[423] Department of Justice, submission dated 29 July 1997, p 35.
[424] American Express, submission dated 1 August 1997, p 2.

effective and uniform regime under a single regulator.[425]

Some private sector submissions argued that privacy regulation was not necessary given that good business practice already demands compliance with privacy guidelines and that the cost of a privacy regime would outweigh any benefits that may flow from its implementation.

The committee's attention was also drawn to various industries which already employ privacy codes of practice. For example, the Bank of Queensland submitted that privacy in the banking industry is adequately protected through measures including the Code of Banking Practice. Thus, the bank submitted that any code or legislation which is implemented should exclude banks (and other commercial entities where applicable) from its operation.

The Australian Bankers' Association submission also discussed in some detail common law and statutory measures protecting privacy in the banking industry, including the Code of Banking Practice and other relevant codes of practice, and concluded that for the banking industry self-regulation was sufficient.

The Queensland Chamber of Commerce and Industry (QCCI) advocated self-regulation for the private sector stating that whilst it, as a matter of principle, supports the concept of privacy protection, it does not agree that the best way to achieve this is by legislation. The QCCI was particularly concerned that all levels of government must minimise regulatory compliance costs and that Queensland with its large concentration of small to medium enterprises is, '*particularly vulnerable to arbitrary regulation where no test of costs or benefits are made*'. Further, the QCCI submitted that the introduction of another layer of legislation and regulation to the day-to-day operations of business would only add to 'red tape'.

With respect to concerns about the enforceability of a self-regulatory system the QCCI responded:

> *The record shows that industry and commerce generally is making every attempt to improve processes of consultation with clients without any compulsion from government due particularly to the need to maintain and/or increase market share and maximise sales. The successful examples of self regulation are those with a clear focus and industry commitment and supervision involving industry association particularly*.[426]

The Institute of Chartered Accountants in Australia (ICAA) favoured a more structured self-regulatory as opposed to legislative system:

> *Privacy legislation would undoubtedly add to the regulatory burden on business and for that reason alone, would be strongly opposed by businesses. Even with a cost/benefit analysis favourable to business, it is likely to still attract significant opposition from the business community. The major difficulty to overcome would be the strong perception that SMEs were, again, being forced to undertake non-productive paperwork for the government.*
>
> …

[425] Australian Bankers' Association, submission dated 30 July 1997, p 8.

[426] Queensland Chamber of Commerce and Industry, submission dated 30 July 1997, p 5.

> *The ICAA recognises that security of personal information may be a growing concern in the wider community. However, we do not consider these concerns would be best addressed by legislative/administrative action. Business should be encouraged to adopt tighter privacy standards in relation to personal data as a sign of best practice. This could best be achieved through voluntary, self-regulatory schemes promoted by industry associations, with the backing and endorsement of the government.*[427]

Thus, the ICAA submitted that in order to show that business strives to exceed customer and staff expectations, business should be encouraged to implement higher standards of privacy protection voluntarily.

However, some private sector organisations did recognise problems with self-regulation. In its submission to the committee American Express commented:

> *While codes have much to commend them as a means of having industry associations address issues specific to their industry there are inherent problems with such an approach. Namely: how non-members in the industry will comply; the level of compliance which can be expected from member companies; what penalties for non-compliance will be put in train; and proof that the industry does in fact deal effectively and appropriately with disputes and recalcitrants.*
>
> *Where such issues can be effectively addressed industry associations can play an important role in having privacy provisions developed which are highly appropriate and designed for each industry.*[428]

10.1.3 Analysis and conclusion

The evidence received by the committee during the course of its public consultation, together with the results of its further research, clearly indicates that there are concerns in the community as to the level of privacy protection afforded to personal information in the private sector. The committee is not convinced that the current law and market processes are adequately addressing these concerns.

In reaching this conclusion the committee has carefully considered the arguments against further information privacy regulation in the private sector which were noted at the outset of this section, and the counter-arguments to these which were addressed by the federal Privacy Commissioner in her August 1997 consultation paper.[429] These counter-arguments include the following.

Firstly, the Commissioner notes that whilst the private sector may not compulsorily require people to provide information, in practice anyone wishing to receive even basic goods and services in Australia today has no choice but to provide information about themselves to the private sector providers of those services.

Secondly, in response to the argument that 'market forces' will adequately protect privacy, the Commissioner states that consumers are unable to select an organisation which they know will adequately protect their information if they do not know what will be done to the information

---

427 Institute of Chartered Accountants in Australia, submission dated 5 August 1997, p 2.

428 American Express, submission dated 1 August 1997, p 10.

429 Federal Privacy Commissioner, August 1997, op cit, pp 4-7.

they provide. In addition, for some organisations the commercial advantages in employing bad privacy practices may outweigh the customer relations of good privacy protection. In other cases consumers may have no real choice as to information privacy practices as they could be standard across an industry.

Finally, whilst recognising that there will be costs associated with the implementation of a scheme, the Commissioner argues that these costs should be reduced by factors such as an adequate phase-in period and the ability for organisations to charge reasonable access costs and to decline unreasonable requests.

The federal Privacy Commissioner also addresses concerns such as those of the QCCI regarding the effect of regulation on Queensland's large number of small and medium-sized enterprises.

> *For a small business with uncomplicated holdings of personal information, compliance costs would be practically nil. Very rarely someone might ask to see payroll or invoice records that relate to them. Apart from that there would be no impact. Responsible businesses in personal information intensive industries already pay attention to privacy issues and, provided there is an adequate phase-in period, compliance costs should be quite manageable; for example, no business would be obliged to reprint millions of forms. The only businesses likely to feel a significant impact are the small minority that are currently handling large amounts of personal information in an irresponsible way, without regard for individuals' wishes or expectations.*[430]

Therefore, the committee believes that the private sector should be subject to further regulation than that which currently applies.

With respect to the issue of what form this additional regulation should take, the committee recognises that there are two main options: a more structured self-regulatory scheme such as that which the federal Privacy Commissioner is currently developing in accordance with the Prime Minister's March 1997 statement, or a legislative scheme such as that initially proposed by the federal Attorney-General in September 1996.

However, there is an overriding factor to be considered before a firm decision can be made with respect to these options. There is a very clear consensus in submissions to the federal Attorney-General's discussion paper, and in submissions to the Commissioner's current consultation process and this committee, that there must be national consistency with respect to a privacy regime for the private sector. It is argued that the promulgation of different privacy regimes by each state and territory would create enormous cost and time inefficiencies for those private sector organisations which have an interstate element to any aspect of their operations.

The committee agrees that, in order to ensure certainty and avoid a patchwork of regulation, national consistency is essential. For example, consider the practical effect of a state-by-state approach on a company which operates in Brisbane but provides services in an area including Tweed Heads and has its national database sourced in its head office in Melbourne.

[430] Ibid, p 6.

On this basis, the committee is supportive of the federal Privacy Commissioner's current consultation process which, most importantly, aims to achieve the objective of national consistency.

This is not to say that the committee has not considered the effect of this process being a self-regulatory scheme. The committee recognises that the arguments against a self-regulatory regime include issues as to lack of enforceability and doubt as to whether such a scheme will provide 'adequate' privacy protection as required by the EU Directive. However, the committee makes two observations in this regard.

Firstly, the issues of implementation with respect to the Commissioner's proposed scheme have yet to be finalised. Therefore, there may be features of implementation mechanisms which overcome some of these concerns.

In her August 1997 consultation paper, the federal Privacy Commissioner states that a self-regulatory scheme is unlikely to be effective without an independent administrator to undertake administrative, coordination and monitoring functions. Therefore, the Commissioner proposes a number of options with respect to ensuring compliance with the scheme and, in particular, canvasses the concept of a scheme administrator. The functions that the Commissioner envisages for this administrator include:

- monitoring whether the objectives of the scheme are being met;
- monitoring whether the scheme is cost effective;
- monitoring whether members are complying with all aspects of the code;
- monitoring whether the scheme is sufficiently adaptable to meet the ongoing needs of its members;
- collecting data such as complaint statistics;
- printing and distributing material about the scheme including the pamphlets relating to the complaint process including bench marking standards;
- monitoring the rate of adoption of the scheme;
- applying or recommending sanctions or penalties against 'free riders' (that is, organisations which do not sign up for the scheme but benefit from the overall perception that they are subject to the scheme); and
- supervising accreditation of organisations which have committed themselves to complying with the scheme.[431]

The Commissioner also notes in that paper that the scheme depends significantly on the provision of accessible, low cost and effective complaint and dispute resolution procedures and that, in the first instance, organisations should be given the opportunity to deal with

[431] Ibid, pp 16-17.

complaints and disputes. The Commissioner canvasses procedures that could be utilised by businesses in this regard.[432]

Secondly, the committee notes the uncertainty as to the potential impact of the EU Directive and the debate as to what is required to meet its terms.[433] The final product of the Commissioner's current process could yet meet the standards of the Directive.

As the federal Attorney-General recently commented regarding the EU Directive:

> *Much is not yet clear about how the directive will operate in practice. However, the EU has not said that privacy legislation is a necessary prerequisite to providing adequate safeguards. Codes of conduct can be relevant to determining adequacy. The directive also permits transfers where safeguards are provided by appropriate contractual clauses and in a number of other circumstances, including where the subject of the data has consented.*[434]

Until such time as some of these issues are clearer, it is difficult to assess the validity of arguments against the current proposed scheme based solely on the EU Directive.

Therefore, at this stage, the committee supports the federal Privacy Commissioner's efforts, in line with the federal government's position, to reach agreement on a national scheme relating to information privacy in the private sector which includes both best practice privacy standards and effective supervisory, enforcement and complaint resolution mechanisms.

10.1.4 Recommendation

Recommendation 25 - The committee recommends that the Queensland government supports the federal Privacy Commissioner's efforts, in line with the federal government's position, to reach agreement on a national scheme relating to information privacy in the private sector which includes both best practice privacy standards and effective supervisory, enforcement and complaint resolution mechanisms.

10.2 PRIVACY IN THE AREA OF HEALTH

10.2.1 Background

Of all personal information held by persons and organisations possibly the most sensitive is information about an individual's physical and mental health. The community therefore generally expects a high level of confidentiality to be afforded to such information.

The committee has already recommended in this report that privacy legislation apply to information held by Queensland government departments and agencies. Whilst this legislation will also apply to health information, the committee has recommended certain modifications to the regime's application in this regard. In particular:

---

432 Ibid, pp 18-20.

433 For a recent article on this debate see Hans van Leeuwen, 'How to beat privacy fears', *The Australian Financial Review*, 20 March 1998.

434 D Williams QC, 'Should we legislate for privacy?', *The Australian*, 5 March 1998.

- in section 6.3 the committee identified health as an area in which there may need to be a code of practice modifying the application of the IPPs;

- in section 6.4 the committee recognised that there should be certain exemptions to compliance with the IPPs. One of the exemptions contained in the principles is where use or disclosure is necessary to prevent threats to life or health. There may also be cases in the context of health in which there should be a public interest exemption. (For example, the sharing of information between certain health providers and the provision of information in the interests of public health.); and

- in section 6.5 the committee recognised that there should be some limits on access to health information; that is, 'retrospective' access should be limited to records of matters of fact and not evaluative material.

In this section the committee focuses on privacy in relation to health information in the *private sector*.

There are a number of reasons advocated as to why privacy legislation should apply to health information held in the private sector as well as the public sector.

Firstly, health information is sensitive regardless of whether it is held in the private or public sector. Therefore, similar principles to that which apply under the *Privacy Act* (Cth) should apply to health information in the private sector. As discussed in chapter 4 of this report, the *Privacy Act* (Cth) applies to a very limited extent to the private sector. In the case of private sector health providers the Act's coverage is limited to hearing service providers.[435] The only other privacy protection offered in the area of health is that provided by the common law duty of confidentiality between doctor and patient and in the medical profession's codes of ethics.[436]

Secondly, as health services are provided by both the public and private sectors, it would be inconsistent for information privacy principles to apply to health information held by public service providers but not to the same information held by their private sector counterparts.

Under the legislative scheme proposed for privacy protection in the private sector by the federal Attorney-General in the 1996 discussion paper *Privacy Protection in the Private Sector*, it was recognised that the question of privacy in the area of health might be addressed by a separate code of practice. However, as already noted, the federal government has announced that it will not be proceeding with a legislative scheme for the private sector.

Such a code has been developed in New Zealand where the Health Information Privacy Code 1994 has been issued under the *Privacy Act* (NZ). This code operates in respect of health

[435] This is as a result of the *Hearing Services and AGHS Reform Act 1997* (Cth) which amended the definition of 'agency' in the *Privacy Act 1988* (Cth) to include 'the nominated AGHS company' or 'an eligible hearing service provider'.

[436] For example paragraph 1.3(D) of the AMA Code of Ethics states: "Keep in confidence information derived from your patient, or from a colleague regarding your patient, and divulge it only with the patient's permission. Exceptions may arise where the health of other is at risk, or you are required by order of a court to breach patient confidentiality." See Dr Bob Brown, Transcript of the committee's seminar on privacy, Brisbane, 17 November 1997, p 9.

information about identifiable individuals and binds a broad range of both public and private health organisations and professionals.[437]

Thirdly, in both the Commonwealth and Queensland public sectors health consumers are granted a right of access to their health information. In addition to access rights under the *Privacy Act* (Cth), FOI legislation in most Australian jurisdictions grants health consumers a right to access certain health information about themselves. (Generally the only exception to this access is in cases where disclosure may be prejudicial to the physical or mental health of the applicant.[438])

In contrast, rights of access in relation to health information held in the private sector are much more limited. In some Australian jurisdictions there are some rights of access in relation to the private sector under miscellaneous statutes. There are also a number of voluntary guidelines in place with respect to access.[439]

The medical profession has also recognised, to some extent, patients' rights of access to records. Revised guidelines on patients' access to records were recently approved by the Federal Council of the Australian Medical Association (AMA). In essence, the guidelines provide that patients have a right to be informed of all *factual* information contained in their medical records relating to their care, but do not have an absolute right to access medical records.[440] The Australian Dental Association Inc also has *a Code of Practice on Patient Information and Records* which includes a section on patients' access to records.[441]

However, these codes and guidelines are voluntary in nature and do not provide persons with a legal right of access. Further, they do not represent comprehensive information privacy principles beyond access as, for example, are contained in the *Privacy Act* (Cth). Doctors are also only one class of a wide range of people who hold health information.[442]

It is also now clear that the common law does not provide private sector health consumers with a right of access to their health information. In the 1995 High Court decision of *Breen v Williams*[443] the court unanimously confirmed that under common law a patient does not have a right of access to inspect or obtain copies of his/her medical records. The decision made it clear that any reform in this area was a matter for the legislature.

---

437 The Health Code also provides individuals or their representatives with a right of access to personal health information. For further discussion on the Code see Longworth and McBride, op cit, pp 87-88 and pp 165-185.

438 See for example s 41(3) of the FOI Act (Cth) and s 44(3) of the FOI Act (Qld).

439 These are noted in a paper by A Cornwall, *Whose Health Records? Attitudes to Consumer Access to their Health Records and the Need for Law Reform*, the Public Interest Advocacy Centre, October 1996, pp 12-15. For example, residents of nursing homes and hostels have special rights under Commonwealth and some state laws. In New South Wales consumers also have a right of access to records held by private psychiatric hospitals.

440 See 'AMA revises medical records guidelines', *Australian Medicine*, vol 9, no 13, July 1997.

441 This Code was adopted by the Federal Council of the ADA at its meeting held on 17/18 April 1997.

442 The federal Privacy Commissioner has noted that, in addition to doctors, other people who hold health records include insurance companies, employers, workers compensation authorities, allied health professionals like physiotherapists, occupational therapists and counsellors and alternative health care providers like chiropractors and homoeopaths. See the Commissioner's second submission to the Senate Community Affairs Committee inquiry into amendments to the Health Insurance Amendment Bill (No 2) 1996, submission no 20, April 1997.

443 (1995-96) 186 CLR 71.

Consumer advocates have for some time argued that patients want access to their medical records for a number of reasons including:

- to gain control of their treatment and their lives;
- to better understand their condition; and
- to check the accuracy of their records.[444]

A number of overseas jurisdictions such as the United Kingdom and most states in the United States have passed legislation granting their health consumers a legal right of access to their medical records.[445] In Canada, the Supreme Court has recognised a common law right for individuals to access their medical records.[446]

Recent developments

There have been a number of recent Australian developments with respect to the privacy of health information in the private sector.

In December 1996, Senator Neal moved an amendment to the Health Insurance Amendment Bill (No 2) (Cth) which sought to create a national right to access medical records. This amendment was subsequently referred to the Senate Community Affairs References Committee for inquiry and report.

In a detailed second submission to that committee[447] the federal Privacy Commissioner proposed that there were a number of criteria for an effective scheme of consumer access to medical records. These included:

- coverage of the full range of privacy issues, that is, not just access;
- coverage of all types of record keepers;
- coverage of all types of health-related records whether or not they are generated in direct connection with the provision of a health service to the individual;
- consistency between the jurisdictions; and
- consistency of standards between the public and private sectors.[448]

On the third point the Commissioner submitted:

> *The sensitivity of the information does not depend on the purpose for which it is created or held. Medical records of great intimacy are created in connection with*

444 Cornwall, op cit, p 4.

445 For some further discussion on this legislation see I Ireland, 'Any change in the Law must be for Parliament' - Breen v Williams and Patient Access to Medical Records', Parliamentary Research Service, Research Paper no 7, 1996-97, pp 16-21.

446 *McInerney v MacDonald* (1992) 93 DLR (4th) 415. As noted above, New Zealand health consumers also have a right of access to their health information under the 1994 Health Information Privacy Code.

447 The Commissioner prepared a second submission because the first preceded the federal government's announcement in March 1997 that it would not be proceeding with privacy legislation in the private sector.

448 Federal Privacy Commissioner, April 1997, op cit, p 5.

> *court cases of various sorts, compensation claims and applications for insurance cover. Developments such as coordinated care, which involve cooperation between State and Territory governments and private and community health workers, entail a health professional coordinating not only a patient's medical needs with other professionals but their social and support needs as well. Technology provides the means for different parts of a person's medical history, in either identified or de-identified form, to be compiled, transmitted, matched, stored and used on a very wide and growing scale, and not necessarily with the patient's free and informed consent*.[449]

Other criteria the Commissioner saw as necessary to an effective scheme included: an enforceable mechanism for resolving disputes about access; a simple, accessible and independent dispute resolution mechanism; systemic protection; exceptions for where access by the individual is inappropriate; and exceptions to disclosure to others.[450]

Accordingly, the Commissioner submitted what she saw as the five main options for protecting the privacy of health information and providing health consumers with a right of access to their health information. In order of the Commissioner's preference (from most to least preferred) these were:

- comprehensive Commonwealth privacy legislation;
- Commonwealth privacy legislation for health information;
- Commonwealth access legislation for the health sector;
- independent legislation by states and territories; and
- a voluntary regime.[451]

The Commissioner explained in her submission that the second of these was, at this stage, the most preferred of the feasible options. (Given that the federal government's announcement of March 1997 had ruled out the first option.)

Thus, with respect to the Commonwealth enacting privacy laws concerning health information the Commissioner stated:

> *Under such laws, individuals would have access and correction rights, subject to appropriate exemptions and conditions; all parties would have legal obligations regarding notification, security and data quality; and there would be strict limits on the use and disclosure of health records by record holders. Organisations interested in personal health information for secondary purposes, such as health funds, would have to obtain the information fairly, and would be limited in how information obtained may subsequently be used or disclosed. Under such a regime, it would be possible for individuals to complain about breaches of the privacy rules to an independent officer with statutory powers, appointed by the government and answerable to Parliament.*

---

449 Ibid.

450 Ibid, pp 6-8.

451 Ibid, pp 9-11. See also the Senate Committee's final discussion on legislative options for the creation of an access scheme in its report, *Access to Medical Records*, Senate Printing Unit, Canberra, June 1997.

> *Such legislation should be flexible in its form. The basic features could be set out in primary legislation but it would be appropriate for matters of detail to be contained in a disallowable legislative instrument in the form of a code of practice developed through wide consultation with stakeholders and the community. Such a structure would allow quicker response to changing circumstances in the sector than detailed provisions in primary legislation, but would still provide an opportunity for consideration by Parliament and wide community consultation.*
>
> *It would be counterproductive if there were major inconsistencies between such a legislated scheme and existing federal, State and Territory FOI statutes which apply to health records held by public sector agencies.*
>
> *It is not certain that the Commonwealth's constitutional powers would allow Commonwealth legislation to reach all parts of the private health sector. If they do not, an effective legislatively based national scheme would require coordinated action by other jurisdictions. It is therefore essential that the States and Territories participate fully in the development of the scheme.*
>
> *This approach would fulfil the criteria of consistency and coverage and would, if appropriately designed, deliver simple and effective dispute resolution mechanisms.*[452]

In relation to the other three options the Commissioner noted the following.

- Commonwealth 'access' legislation is not preferred as it only deals with access. Access to records is integrally related to other aspects of information privacy and all of these aspects should be addressed simultaneously.
- Independent legislation by the states and territories [in relation to either (preferably) information privacy protection in general, or access to health records] would most likely lead to inconsistency between the various jurisdictions.
- A voluntary regime has a number of disadvantages. In particular, it may not provide people with adequate opportunity to complain about and be compensated for breaches, and would not provide people with any legal right to gain access to information held by private sector health care providers.[453]

In June 1997, the Senate committee tabled its report *Access to Medical Records*. In this report the majority of that committee recommended, amongst other matters, that national legislation enshrining the right of access to medical and other health records in the private sector be drafted without delay. The majority also recommended that this be done through the creation of extended privacy legislation and that it be carried out to avoid conflicting state and territory access to medical and other health records legislation.[454]

However, despite this recommendation for a national approach, in December 1997 the ACT Legislative Assembly passed the *Health Records (Privacy and Access) Act*[455] which protects the privacy of personal health information held by both the public and private sectors. The Act

---

452 Ibid, pp 9-10.

453 Ibid, pp 10-11.

454 Senate Community Affairs References Committee, op cit.

455 The Act followed an ACT government position paper, *Health Records: Privacy and Access*, ACT Government Printer, May 1997.

does this by implementing IPPs consistent with those that currently appear in s 14 of the *Privacy Act* (Cth), albeit modified to suit the health sector. The Act also gives health consumers rights of access in relation to their health information. In the case of records that contain factual matters this right exists regardless of when the record was made. However, the right only applies to the extent that a health record contains matters of opinion, to records created on or after the date of commencement of the Act.[456]

The issue of access to medical records was also considered by the ALRC/ARC joint review of the FOI Act (Cth).[457] Although that review rejected the notion of extending FOI legislation to the private sector, it did consider that the *Privacy Act* (Cth) could be extended in relation to access to medical records. Moreover, the review noted the desirability for the question of access to be dealt with on a national basis.

> *The review considers that access to health and medical records in the private sector could be dealt with in the context of a comprehensive national privacy regime. The importance of the issue points to the need for a national regime to be implemented quickly.*[458]

Other privacy issues in the area of health have been raised in a number of other contexts. For example, privacy issues were raised in the inquiry by the House of Representatives Standing Committee on Family and Community Affairs into Health Information Management and Telemedicine.[459]

The recent proposal by the federal government to link pharmacies through a national computer system to collect, collate, and hold information derived from patient prescriptions has also raised issues as to patient confidentiality.[460]

10.2.2 Arguments raised in public consultation

The committee received a number of submissions from health providers and health-related organisations. These submissions recognised that there are particular areas of concern with respect to privacy and health which need to be addressed by legislative and/or administrative action.

The Prince Charles Hospital listed some of the most pressing concerns to be addressed in the area of health to be:

- protection of patient confidentiality;
- authorisation of access to users and potential users of confidential patient information or data;
- managing privacy of patient information in the transition from a paper-based to an electronic/computer-based system including:

---

456 See s 10.

457 ALRC and ARC, op cit.

458 ALRC and ARC, op cit, pp 207-208.

459 Parliament of the Commonwealth of Australia, House of Representatives Standing Committee on Family and Community Affairs, *Health on line: A Report on Health Information Management and Telemedicine*, Australian Government Publishing Service, Canberra, October 1997.

460 See the article 'Chemists' computer link-up row', *The Courier-Mail*, Brisbane, 3 November 1997, p 5.

  - creation of health information databases
  - linkages between and among health information databases
  - specification and use of a unique patient identifier
  - information system design and implementation standards for storage and transmission of sensitive medical data
  - information systems policy for health information
  - access control mechanisms to address security risks
  - information audit trail or tracking
  - defences against electronic misappropriation of health information
- mechanisms for enforcing breaches of patient confidentiality by primary, secondary or third party users;
- guidelines or regulations for non-direct patient care users of patient data in both the public and private sector;
- informed consent from patients to use their health information;
- patient access to their own medical/clinical records;
- access by relatives and other parties including legal professionals to clinical records; and
- policies and procedures to protect patient's privacy in telemedicine activities.[461]

The Queensland Nurses' Union noted a number of similar concerns.

Accordingly, these and other submissions recommended further legislative protection in the area of health in both the public and private sectors.[462]

The committee also received evidence at its public hearing in Townsville from Dr Tony Landgren, Director of Medical Services, Mater Private Hospital. Dr Landgren is both a doctor and a lawyer and he raised a number of issues with respect to privacy in the private health sector including:

- the practical difficulties in separating health information from other information such as financial information, much of which is subject to confidentiality agreements without outside bodies;
- problems as a result of the hospital being obliged to disclose information in relation to health complaints to certain organisations which are in turn subject to FOI. The difficulty for the hospital in these cases is that they have an arrangement with their

[461] The Prince Charles Hospital and Health Service District, submission dated 30 July 1997, p 5.

[462] Refer to the submissions received from The Prince Charles Hospital and District Health Service, the Queensland Nurses' Union and the Royal Australian College of Medical Administrators.

insurers not to disclose patient information in this type of circumstance without the consent of the insurer;

- compliance costs in separating information which is necessary because both the private organisations it deals with and also government organisations are increasingly requiring the hospital to disclose information. Whilst the hospital has reasonable systems in place to note to whom they have disclosed what information, there is always a risk associated with that, and trying to obtain insurance to protect hospitals from unintentional disclosure of information is almost impossible[463]; and

- problems in applying a self-regulatory or legislative scheme to old records, particularly considering that many older records contain information in relation to medical practitioners' thought processes or personal views. Therefore, he submitted that for any scheme to be workable it probably has to apply prospectively in a general sense and selectively retrospectively.[464]

At the committee's seminar on privacy Dr Bob Brown, the President of the AMA (Queensland), picked up on this last point regarding access to information.

> *Public hospital records are available through freedom of information and other means to patients. It is the belief of the AMA that factual information of the patient's private medical records should be made available to the patient on request, but under certain circumstances which would allow the doctor to explain to the patient the detail and relevance of the records of history, examination, investigation and diagnosis, all of which is factual, as well as a plan of management.*
>
> *The AMA believes that the other part of the medical records which we as doctors think to be separate, which may be regarded as an aide-memoire and may include the deductive processes as well as other information, say, obtained from a patient's relative, spouse or friend, as does happen in general practice in particular, is the property of a doctor and, as such, should be protected by legislation. Likewise the release of patient records to a third party without the permission of the patient should be under the circumstances of being in the public good, as mentioned earlier, or by court order, as may occur by subpoena or a writ of third-party discovery*[465].

Dr Brown also canvassed the issue of required disclosure to third parties and the proposal to link-up pharmacies by computer:

> *Linked to the issues of confidentiality and access to patient records is the release of information to third parties other than the court, and this includes Government and its instrumentalities, insurance companies and other professional groups. Of*

---

463 In this regard Dr Landgren stated that he believes the health sector could be covered under general legislation on privacy but he stressed that privacy and required disclosure are two different areas which will have to work together in an integrated way. Whilst Dr Landgren submitted that a code of conduct for medical practitioners regarding disclosure would be very easy, he also stated that the difficulty which arises is that such a code would not apply to the insurance industry. Dr Landgren believes that it would be possible for the health and insurance industries to agree on a workable code of conduct and that this would be in the interests of the insurance industry as the costs in maintaining the current arrangements are huge.

464 Transcript of the committee's public hearing, Townsville, 14 November 1997, pp 17-20. Dr Landgren's comments with respect to 'retrospective' access have already been noted in relation to health information held by the public sector.

465 Transcript of the committee's public seminar on privacy, Brisbane, 17 November 1997, p 9.

> *particular concern to the AMA is the ever-increasing information gathering of the Health Insurance Commission, and a new pilot study recently announced by Dr Wooldridge initiated by the Pharmacy Guild which plans to link pharmacies through an Intranet to collect, collate and hold information derived from patient prescriptions. Although there are several attractive and beneficial possibilities, at this time the AMA is concerned about the potential for breach of privacy and confidentiality and is continuing a watching brief. This is but an example of the perceived need for more and more information, but with the potential for the loss of personal freedom and privacy.*[466]

10.2.3 Analysis and conclusion

The committee believes that specific consideration needs to be given to all aspects of information privacy regarding health information, including health consumers' access rights. This is evident from the recommendations that the committee has already made with respect to information privacy legislation to apply to health information in the public sector.

However, as the submissions to the committee support, there are sound reasons as to why health information in the private sector should also be given specific consideration. In particular, the committee notes:

- the inconsistencies that will arise if comprehensive privacy legislation is introduced to cover Queensland's public sector but not the private sector given that health and medical services are provided in both the public and private sectors; and

- the need to reconcile the different standards that currently apply to accessing health information in the public and private sectors (as access under FOI legislation applies only to public sector health services and following the recent decision of *Breen v Williams* it is clear that there is no common law right of access to health information held in the private sector).

The above background discussion reveals that there is a large body of support for privacy legislation covering health information in both the public and private sectors. In particular, this support is from the federal Privacy Commissioner and the Senate Community Affairs References Committee.

Given the federal government's announcement that it will not be legislating in relation to privacy in the private sector, the options for Queensland with respect to protecting the privacy of personal health information and providing health consumers with a right of access to their health information are to:

- urge the Commonwealth to pass privacy legislation regarding the privacy of health information, or achieve a similar result through a co-operative state and territory scheme which will avoid constitutional uncertainties;

- pass specific 'state' privacy legislation in relation to health such as that recently passed in the ACT; or

[466] Ibid, p 10.

- support the federal Privacy Commissioner's current self-regulatory scheme in relation to privacy in the private sector in general. (Although, admittedly, this option would still not give health consumers a *legal* right of access to their health information.)

In weighing up each of these options the committee has again been particularly mindful of an overriding consideration which the Commissioner has made clear; namely, that as far as possible national consistency is desirable. The Commissioner's reasons in this regard (as stated in her submission to the Senate Committee) are as follows.

> *First, different schemes in different jurisdictions would make for complexity and confusion. For example, people frequently move from State to State; a person may seek treatment for the same condition in more than one jurisdiction; and it would be anomalous if records were available for one treatment episode but not another.*
>
> *Second, the sensitivity of health records and the damage that inaccurate, misleading or mishandled records can inflict on an individual, do not differ from jurisdiction to jurisdiction. Wherever in Australia a person's health records are held, equity demands that they have an appropriate level of access to those records.*
>
> *Third, different standards in different jurisdictions are likely to increase the costs of compliance for organisations that operate across State boundaries. Pathology laboratories, chains of private hospitals and national health insurers, for example, would need to become familiar with a different set of standards and procedures in each jurisdiction.*[467]

In its report, the Senate Community Affairs References Committee concluded after discussing the ACT's then proposal for separate health privacy and access legislation:

> *The Committee is of the view that national legislation is preferable to separate State and Territory legislation. National legislation would bring all States and Territories on line simultaneously, removing any inconsistencies or uncertainties in rights of access.*[468]

The committee has already commented in the previous section about the need for national consistency when it comes to regulating information privacy in the private sector generally. For the same reasons as stated previously and noted above, the committee agrees that regulation of the private sector with respect to health information should be also done on a nationally consistent basis.

The committee notes that the Commissioner's recently released *National Principles for the Fair Handling of Personal Information* in the private sector have been framed in general terms so that they may be applied to a wide range of industries, professions and organisations. These principles can be adopted by private sector health providers and other persons and organisations that collect and use health information.

Therefore, just as the committee has recommended that the IPPs proposed for Queensland's public sector may need to be modified in the area of health, most likely the Commissioner's

---

467 Federal Privacy Commissioner, April 1997, op cit, p 6.

468 Senate Community Affairs References Committee, 1997, op cit, p 76, para 5.17.

national principles will also need to be modified to apply specifically to persons and organisations which collect, hold and use health information in the private sector.[469]

Given the desirability to avoid a patchwork of state and territory approaches to the privacy of health information in the private sector, the committee believes that the Queensland government should not legislate or take further action in this area at this stage. This approach will also enable an assessment to be made as to the outcome of the federal Privacy Commissioner's consultation regarding issues associated with the implementation of the 'national principles', and the overall success of the scheme in which those principles will operate.

10.2.4 Recommendation

Recommendation 26 - The committee recognises that specific consideration needs to be given to issues associated with the privacy of health information, particularly in the private sector. However, it also recognises that any regulation in this regard should be nationally consistent.

Therefore, the committee recommends that the Queensland government supports the federal Privacy Commissioner's efforts, in line with the federal government's position, to reach agreement on a national scheme relating to information privacy in the private sector which includes both best practice privacy standards and effective supervisory, enforcement and complaint resolution mechanisms in all areas including health.

However, the committee also recommends that, once established, the Queensland Privacy Commissioner review the privacy protection afforded to health information in the private sector as a result of that scheme, and make any necessary recommendations for change.

[469] In her letter dated 21 November 1997 the Commissioner noted that whilst there was a consensus that there only be one set of principles, it was also noted that there may be a need to modify the principles through the implementation of some industry specific codes, such as a Health Code.

PART 4

11. CHAPTER 11 - OTHER SPECIFIC INFORMATION AND NON-INFORMATION PRIVACY CONCERNS

11.1 INTRODUCTION

As explained at the outset of this report, the committee did not want to unduly limit the privacy areas or issues that submissions to its inquiry might address. Accordingly, the committee's issues paper canvassed a broad range of privacy concerns in order to gauge public sentiment on an array of matters.

In this report, the committee has already addressed many concerns raised in public submissions[470] by recommending that Queensland introduce a Privacy Act enshrining information privacy principles to apply, at least initially, to Queensland government departments, agencies, government contractors and GOCs. The committee has also recommended and that an office of Queensland Privacy Commissioner be established to oversee compliance with the IPPs and the operation of the Act. By doing this, a privacy framework has been proposed for Queensland.

In this chapter, the committee deals with some additional matters which may, or may not, fit within this framework. In sections 11.3 to 11.6, the committee discusses some specific areas in which the community clearly has privacy concerns.[471] These areas are:

- surveillance;
- smart cards and electronic commerce;
- the use of genetic information; and
- the news-gathering and reporting activities of the media.

However, to introduce these issues, the next section of this chapter (section 11.2) discusses two wider considerations that the just-mentioned issues raise; namely:

- the capacity of the proposed privacy regime to address privacy issues that may become areas of public concern in the future; and
- the capacity of the proposed privacy regime to deal with *non-information* privacy concerns.

---

470 Section 1.4 of this report lists the wide range of matters that arose in public submissions.

471 Other specific privacy concerns fall within areas already canvassed by the committee. For example, direct marketing, telemarketing and the operation of tenancy databases is canvassed within the discussion in chapter 10 (privacy regulation in the private sector). The use, access and disclosure of health and medical records is also discussed in chapter 10 (regarding the private sector) and in chapter 6 (regarding the public sector). Special cases for law enforcement and other discrete privacy areas are also discussed in terms of either becoming subject to codes of practice issued by the Privacy Commissioner (in section 6.3) or exemptions to compliance with the IPPs (section 6.4).

11.2 THE CAPACITY OF THE PROPOSED PRIVACY REGIME TO ADDRESS FUTURE PRIVACY CONCERNS AND NON-INFORMATION PRIVACY CONCERNS

11.2.1 Background

There is no doubt that discrete subject areas affecting individuals' privacy will develop as areas of public concern in the future. This is already evident from commentary on relatively recent technological developments like the Internet, digital cash, multi-application smart cards and potential uses for biometric information. A question arises, then, as to what extent the committee's proposed privacy regime will be able to recognise and deal with new privacy issues as they come about, particularly those stemming from the development of technology.

A second issue also arises. The focus of the regulatory regime proposed by the committee thus far has been on protecting *information privacy* in a general sense. However, areas of public concern such as surveillance and the news-gathering and reporting activities of the media, at least to some extent, involve *non-information* privacy concerns. As discussed later in this chapter, surveillance of itself (without associated recording of the personal information of the individual(s) being targeted) does not involve information privacy. Likewise, journalists invading the privacy of a newsworthy individual's personal space when gathering information does not involve information privacy. Therefore, this second issue is about the ability of the committee's proposed privacy regime to address issues of *non-information* privacy.

Both of these issues were a recognised in an article introducing the Australian Privacy Charter Council's Privacy Charter:

> *The privacy debate now goes beyond information privacy issues into issues of surveillance, communications and other technology issues. Information privacy remains the prominent issue in privacy protection, with developments such as the Internet, computer-matching and profiling in recent years. But a range of other developments, including smart cards, biometric identification, genetic testing, and surveillance technologies have widened the scope of debate over the right to privacy.*
>
> …
>
> *The Privacy Charter establishes that the scope of the right to privacy expands well beyond data protection. Principles 6 to 9 of the Charter include a right to freedom from surveillance, privacy of communications, private space, and freedom from interferences with physical privacy. The provisions address a range of new technological applications which have the potential to affect the individual's right to privacy.*[472]

To a certain degree, both of these issues are satisfied by the broader functions that the committee has already recommended for the Queensland Privacy Commissioner.[473]

These broad functions include:

- examining (on the Commissioner's own volition or as requested) proposed legislation that might entail interferences with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals and ensuring that such effects are

[472] T Dixon, 'Privacy Charter sets new benchmark in privacy protection', *Privacy Law and Policy Reporter*, vol 2, no 3, April 1995, pp 41-45, p 42.

[473] These functions largely mirror the functions of the federal Privacy Commissioner.

minimised [mirroring the *Privacy Act* (Cth), s 27(1)(b)];

- researching and monitoring technological developments to ensure that any adverse effects of such developments on the privacy of individuals are minimised [s 27(1)(c)];
- publishing guidelines for the avoidance of acts or practices of an agency that may or might be interferences with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals [s 27(1)(e)];
- providing advice (with or without a request) to a Minister or an agency on any matter relevant to the proposed Privacy Act [s 27(1)(f)];
- conducting education about individuals' privacy [s 27(1)(m)];
- doing anything incidental or conducive to the preceding functions [s 27(1)(o)]; and
- reporting on any matter that concerns the need for, or the desirability of, legislative or administrative action in the interests of the privacy of individuals [s 27(1)(r)].

These wider functions of the Queensland Privacy Commissioner would give the Commissioner some capacity to deal with information privacy issues that develop in the future.[474] However, the capacity of the Queensland Privacy Commissioner to address *non-information* privacy concerns, either now or in the future, is not as clear.

As stated in this report, the Privacy Act (Qld) is to broadly model its IPPs and the functions of the Queensland Privacy Commissioner on those contained in the *Privacy Act* (Cth). The Commonwealth *Privacy Act* does not explicitly state that the federal Privacy Commissioner has functions in relation to privacy other than *information privacy*. Indeed, Tucker's 1992 book, *Information Privacy Law in Australia*, states that the Commonwealth Act '*affords protection for information privacy only*'[475] and that, because of this, the title of the *Privacy Act* is misleading.[476]

The basis for this contention is s 13 of the *Privacy Act* (Cth). Section 13 provides that an act or practice is an '*interference with the privacy of an individual*' *if, and only if* - in the case of an agency - the act or practice breaches an IPP in relation to personal information that relates to the individual.[477] Some of the functions of the federal Privacy Commissioner listed above that most appear to increase the scope of the Commissioner's jurisdiction contain the phrase '*interferences with the privacy of individuals*'. Thus, not only are the IPPs by definition restricted to information privacy but some of the apparently wider functions of the Privacy Commissioner are seemingly - via the operation of s 13 - restricted to information privacy.

---

474 As would the inherent flexibility of the IPPs proposed for Queensland, both in terms of the fact that these IPPs are broad in nature and because the committee proposes that they can be modified to suit a specified agency, activity, information, etc through codes of practice.

475 G Tucker, op cit, p 75.

476 Ibid, p 76.

477 'Agencies' are covered by s 13(a). Section 13 also provides other instances of '*interferences with the privacy of an individual*' by other entities, none of which expand the limited definition of that phrase in s 13(a).

Arguably, on a wider reading of those functions, this may not be the case.[478] Nevertheless, the restrictions placed on the federal Privacy Commissioner by the *Privacy Act* (Cth) in relation to non-information privacy matters (at least in the form of visual surveillance) is apparent in the following excerpt from the Privacy Commissioner's guidelines on *Covert Optical Surveillance in Commonwealth Administration*:

> *Where covert surveillance results in the creation of some kind of personal information concerning an individual, the activity, if undertaken by Commonwealth agencies is regulated by the Privacy Act. In the situations where the covert surveillance does not lead to the creation of a record, agencies, while not bound to comply with the Privacy Act, are encouraged to adopt the following guidelines where relevant.*[479]

11.2.2 Arguments raised in public consultation

The majority of submissions received by the committee stressed that a privacy regime should contain mechanisms to monitor developments in technology and data management and to review new procedures that might threaten individuals' privacy. As the CJC pointed out, '*The dynamic nature of technology capable of storing and disseminating information clearly requires constant review of the implications of that technology for privacy.'* As noted above, such technological developments have ramifications for non-information privacy as well as information privacy.

Relevantly, as the federal Privacy Commissioner submitted to the committee:

> *One of the strengths of general privacy principles is that they should be capable of application to any technology. This at least provides a permanent framework in which may address the privacy implications of a new technology or a new application of an existing technology.*[480]

Nevertheless, the federal Privacy Commissioner made the following concomitant observation:

> *But broad principles alone will not ensure that all privacy issues are adequately addressed. In specific contexts, specific measures may be needed and this requires some mechanism for identifying emerging information privacy issues and feeding them into the policy making process ... [O]ne of the functions of the Privacy Commissioner or Privacy Committee should be to monitor the privacy implications of technological developments.*[481]

---

478 The phrase '*interferences with the privacy of individuals*' in those wider delineated Commissioner functions [at any rate since a 1990 amendment to the *Privacy Act* (Cth)] is followed by the phrase '*or which may otherwise have any adverse effects on the privacy of individuals*'. This may have the effect of widening the relevant Commissioner functions to extend beyond the *information* privacy of individuals. The *Data-Matching Program (Assistance and Tax) Act 1990* amended subsections 27(1)(b), (c), (e) and (k) of the *Privacy Act* (Cth) by adding '*or which may otherwise have any adverse effects on the privacy of individuals*'.

479 Privacy Commissioner, *Covert Optical Surveillance in Commonwealth Administration: Guidelines*, Privacy Commissioner, Sydney, February 1992, p 7.

480 Federal Privacy Commissioner, submission dated 26 August 1997, p 17.

481 Ibid.

The Queensland Council for Civil Liberties submitted:

> *It should be a clear requirement on a Privacy Commissioner/Committee to research privacy issues both in Australia and overseas, and to put forward proposals for reform (as well as drafting appropriate subordinate legislation) in response to developments in technology, changes in societal expectations and the changing requirements of government and the workplace.* [482]

Submissions also generally suggested that any privacy commissioner or committee should have a function in relation to discrete information privacy concerns (for example, direct marketing and privacy of employment records), and non-information privacy concerns (for example, surveillance generally and use of genetic information in a wider sense).

The Anti-Discrimination Commission (Queensland) submitted that:

> *... issues such as advancing technology (e.g. smart cards), surveillance and data matching, these are complex matters which only serve to highlight the need for a strong privacy legislative regime, oversighted by a Commissioner with broad policy and consultative functions. Once in place, a Privacy Commissioner could establish priorities and commence a process of consultation and research to determine the most appropriate response to these issues.*[483]

11.2.3 Analysis and conclusion

In relation to *discrete information privacy* concerns that currently exist or that may develop in the future, the committee reiterates that the IPPs and the functions of the Privacy Commissioner proposed earlier in this report would enable the Commissioner to deal with specific information privacy issues as the Commissioner thinks appropriate. However, as identified in public submissions, the Privacy Commissioner should also be responsible for monitoring future developments for any adverse privacy implications.[484] As stated by the ADC-Q and the QCCL, issues such as advancing technology, changes in societal expectations and changes in government and workplace requirements suggest that the Queensland Privacy Commissioner should have broad consultative and research functions to help determine the most appropriate responses to such matters.[485]

The second issue raised by the committee in this section was whether the Queensland Privacy Commissioner has, or should have, the capacity to address privacy concerns that do not relate to information privacy.

The regime proposed so far by the committee for Queensland, because it is based in many respects on the *Privacy Act* (Cth), is arguably restricted to handling matters of *information privacy*. This is appropriate *with respect to the IPPs* (by definition, the IPPs are restricted to information privacy) and with respect to the Commissioner's functions that directly concern the IPPs and information privacy.

---

482 Queensland Council for Civil Liberties, submission dated 12 August 1997, p 17.

483 Anti-Discrimination Commission (Queensland), submission dated 1 August 1997, p 7.

484 This is a function already recommended for the proposed Queensland Privacy Commissioner in chapter 7.

485 It was noted in chapter 2 that privacy is a difficult concept to define for reasons including that the concept of privacy changes (in accordance with not only developments in technology but also society's values and expectations). A 'Privacy' Commissioner should be able to respond to these changes.

However, the committee does not believe that the entire regime should be limited to dealing with information privacy. In particular, the committee believes that the Queensland Privacy Commissioner's broader functions should not be limited to dealing with information privacy concerns. Even if the federal Privacy Commissioner's functions, as listed in s 27(1) of the *Privacy Act* (Cth), do enable the federal Commissioner to deal with non-information matters to some extent, the committee is strongly of the opinion that the proposed privacy legislation should make it explicit that the Queensland Privacy Commissioner is capable of addressing non-information privacy concerns.

The Queensland Privacy Commissioner should be able to monitor practices such as visual surveillance activities that are undertaken by agencies and have ramifications for the privacy of individuals but do not necessarily involve 'information privacy'. The committee does not believe this would detract from the emphasis of the Privacy Act (Qld) on information privacy.

Therefore, the committee believes that the Privacy Act (Qld) should make it clear that the Commissioner is responsible for addressing non-information privacy concerns (along with information privacy concerns) when the Commissioner undertakes the (wider) functions listed in section 11.2.1 above; namely, the functions in relation to:

- examining proposed legislation [mirroring the *Privacy Act* (Cth), s 27(1)(b)];
- researching and monitoring technological developments [s 27(1)(c)];
- publishing guidelines for the avoidance of privacy-intrusive acts or practices of an agency [s 27(1)(e)];
- providing advice to a Minister or an agency on matters relevant to the Act [s 27(1)(f)];
- conducting education [s 27(1)(m)];
- doing anything incidental to the preceding functions [s 27(1)(o)]; and
- reporting on matters that concern the need for, or the desirability of, legislative or administrative action [s 27(1)(r)].

Extending the parameters of the above functions of the Queensland Privacy Commissioner so that the Commissioner can address non-information privacy matters as well as information privacy matters would broaden the Commissioner's mandate to effectively deal with a wider range of privacy issues. It would also remove possible artificial distinctions from the Commissioner's jurisdiction. The Commissioner would not first have to ensure, for example, that 'personal information' is actually involved before the Commissioner examines proposed legislation, or looks into new technologies or legislative proposals that might be privacy-intrusive.[486]

The Committee notes that the functions of the New South Wales Privacy Committee are not restricted to dealing with matters involving information privacy under the *Privacy Committee Act 1975* (NSW). Some of the wider functions of the Privacy Committee are similar to that of

[486] The wording of the Commonwealth *Privacy Act* (on which the proposed Queensland Privacy Act is based), would need to be modified when drafting either the 'functions' provisions of the Queensland Act [the equivalent of s 27(1)] or when drafting the s 13 equivalent affecting the interpretation of various functions.

the federal Privacy Commissioner. For example, the committee may report to the Minister with recommendations in relation to any matter that concerns the need for, or the desirability of, legislative or administrative action in the interest of the privacy of persons.[487] However, 'privacy of persons' is not restricted in the *Privacy Committee Act* by a definition referring to 'personal information'.

On the matter of extending to non-information matters, the function of the Queensland Privacy Commissioner in relation to issuing guidelines for the avoidance of privacy-intrusive acts [based on s 27(1)(e)], the committee notes that any ensuing guidelines would not be binding on the subject agencies. It might be that, once the Act had been in place for some time, the nature of the guidelines could be revisited. If it would enhance the efficacy of the regulatory system, moves could be made to make such guidelines binding on agencies. However, the committee believes that any ensuing guidelines should only be issued by the Queensland Privacy Commissioner after consultation with stake-holders and that such guidelines should be published in the form of disallowable instruments.[488]

11.2.4 Recommendation

Recommendation 27 - The committee believes that, while the IPPs themselves and the functions of the Queensland Privacy Commissioner that relate directly to the IPPs and information privacy should be restricted to information privacy matters, the Queensland Privacy Commissioner should explicitly be given jurisdiction to deal with non-information privacy concerns.

Accordingly, the committee recommends that the parameters of the following functions that were recommended for the Queensland Privacy Commissioner in chapter 7 of this report be extended to enable the Commissioner to address non-information privacy matters (that is, matters that involve no record of personal information):

- **examining proposed legislation [mirroring the *Privacy Act* (Cth), s 27(1)(b)[489]];**
- **researching and monitoring technological developments [s 27(1)(c)];**
- **publishing guidelines for the avoidance of privacy-intrusive acts or practices of an agency [s 27(1)(e)];**
- **providing advice to a Minister or an agency on matters relevant to the Act [s 27(1)(f)];**
- **conducting education [s 27(1)(m)];**
- **doing anything incidental to the preceding functions [s 27(1)(o)]; and**

---

487 *Privacy Committee Act 1975* (NSW), s 15(b). The committee may also report, under s 15(c), to any person in relation to any matter that concerns the need for or the desirability of action by that person in the interests of the privacy of persons.

488 The process the committee proposes for developing codes of practice in relation to the IPPs may provide some useful guidance in this respect.

489 In chapter 7, the committee recommended that the functions of the Queensland Privacy Commissioner should be broadly modelled on those contained s 27 of the *Privacy Act* (Cth).

- **reporting on matters that concern the need for, or the desirability of, legislative or administrative action [s 27(1)(r)].**

This will ensure that the Queensland Privacy Commissioner has the capability to address both information and non-information privacy concerns that may arise in the future.

11.3 SURVEILLANCE

11.3.1 Background

Surveillance (when no record of personal information is made) is one of the non-information privacy areas referred to in the last section. Surveillance is the monitoring of the movements or activities of a person. Surveillance can involve a number of dimensions. It can be:

- physical (watching a person), electronic (via equipment such as listening devices, cameras, closed circuit television, telecommunications interception devices or location tracking devices),[490] or online (through the target's computer activities)[491];
- covert or overt[492]; or
- visual, aural or both.

While the particular privacy ramifications of surveillance differ depending on the type of surveillance being utilised, the Australian Law Reform Commission has stated that, generally:

> *…the intentional surveillance of an individual's activities or conversations can have a corrosive effect on [the individual's] sense of privacy and is generally considered as a serious affront to the integrity of the individual subjected to this practice.*[493]

The Australian Law Reform Commission explained why the existing law concerning surveillance is lacking:

---

490 Forms of *electronic surveillance* are discussed by the Criminal Justice Commission in its *Report on a Review of Police Powers in Queensland - Volume V: Electronic Surveillance and Other Investigative Procedures*, Queensland Government Printer, Brisbane, October 1994, p 749.

491 For the issues raised by online surveillance, see S Miller, 'Privacy and the Internet', *Australian Computer Journal*, vol 29, no 1, February 1997, pp 12-15. For other, highly technical forms of surveillance, see B Mason, 'Privacy and law enforcement in Queensland: A two-faced Big Brother?', *Themis*, vol 2, no 3, November 1997, pp 36-41; T McBride, 'State surveillance: the slippery slope? Recent examples of the emerging surveillance society in New Zealand', *Privacy Law and Policy Reporter*, vol 4, no 4, September 1997, pp 71-74.

492 Covert surveillance is carried out by concealed devices without the notice of the subject being targeted. Overt surveillance involves monitoring the movements of people that have been given notice of the surveillance or are aware of the surveillance in a general sense, but are not aware that any particular behaviour is being monitored at any given moment: New South Wales Law Reform Commission, *Issues Paper 12: Surveillance*, Law Reform Commission, Sydney, May 1997, p 7; R Simpson, *Listening Devices and Other Forms of Surveillance: Issues and Proposals for Reform*, Briefing Paper No 20/97, New South Wales Parliamentary Library, November 1997, p 2.

493 Australian Law Reform Commission, *Discussion Paper: Privacy and Intrusion*, AGPS, Sydney, 1980, as cited in federal Privacy Commissioner, *Covert Optical Surveillance in Commonwealth Administration: Guidelines*, Privacy Commissioner, Sydney, February 1992, p 1.

> *...technological developments have given rise to sophisticated devices which render it virtually impossible for the ordinary person to take effective measures against the use of technological devices. The ancient statutory offence of peeping and the common law crimes of eavesdropping sought to restrain deliberate surveillance. But each of these were created long before the modern development of sense-enhancing technical services. As the law currently stands there is insufficient legal protection against the use of these devices. They have proliferated. The law has not kept pace.*[494]

The committee's issues paper asked what form of regulation should be introduced to deal with privacy issues arising from surveillance.

To the extent that a Queensland government department or agency undertaking surveillance records personal information, the privacy regime being proposed by the committee would apply to that resultant information.[495] Therefore, IPP 1, for example, would dictate that the information arising from the surveillance must be collected for a lawful purpose directly related to a function or activity of the collector. IPP 1 would also demand that it was not collected by unlawful or *unfair* means. IPP 3 would demand that the person undertaking the surveillance take reasonable steps to ensure that, amongst other things, the information collected was complete and directly relevant to the purposes of its collection. Other IPPs would apply to protect the information once recorded.[496]

However, surveillance goes beyond issues of *information* privacy (as noted above) and the IPPs would not necessarily apply to surveillance activities.[497] Further, surveillance adversely affects privacy *per se*. The Australian Privacy Charter Council recognised this by including in their Privacy Charter the following privacy principle.

> ***6. Freedom from Surveillance***
>
> *People have a right to conduct their affairs free from surveillance or fear of surveillance. 'Surveillance' means the systematic observation or recording of one or more people's behaviour, communications or personal information.*[498]

The New South Wales Law Reform Commission has recently stated:

> *However, there is no necessary connection between surveillance and the collection of information. As surveillance is considered intrusive in itself, regardless of any information-collecting purpose, mere regulation of the use of information obtained by surveillance is likely to be considered insufficient protection of privacy.*[499]

Surveillance and Law Enforcement

Covert surveillance of all types is predominantly used for law enforcement purposes where the person targeted is suspected of being involved in criminal activity. In Queensland, covert surveillance is used by the Queensland Police Service (QPS) and the Criminal Justice

494 ALRC, 1980, op cit, cited in federal Privacy Commissioner, ibid, p 4.

495 See the discussion in section 11.1 of this report.

496 Certain exceptions in relation to law enforcement and other matters would also apply. These exceptions are canvassed in section 6.4 of this report.

497 See generally G Greenleaf, 'Stopping surveillance: Beyond "efficiency" and the OECD', *Privacy Law and Policy Reporter*, vol 3, no 8, December 1996, pp 148-152.

498 Australian Privacy Charter Council, *Australian Privacy Charter*, December 1994.

499 New South Wales Law Reform Commission, op cit, p 13.

Commission (CJC). It can also be used by Commissions of Inquiry and is envisioned to be used by the recently established Queensland Crime Commission (QCC). In addition, federal agencies operating in Queensland such as the Australian Federal Police, the National Crime Authority and Australian Security Intelligence Organisation (ASIO) also utilise covert surveillance.[500]

Apart from the *Invasion of Privacy Act 1971* (which makes it an offence to use a listening device to record or listen to a private conversation),[501] Queensland legislation that deals with surveillance undertaken by law enforcement agencies is the *Drugs Misuse Act 1986*, *Criminal Justice Act 1989*, *Commissions of Inquiry Act 1950*, *Queensland Crime Commission Act 1997* and the *Police Powers and Responsibilities Act 1997*.[502] The Queensland government also recently introduced into the Legislative Assembly the *Telecommunications (Interception) Queensland Bill 1998*[503] to give the QPS, CJC and the QCC the power to intercept phone calls.[504]

Other uses of surveillance

Overt visual surveillance [usually in the form of closed circuit television (CCTV)] is increasingly being used in public places. For example, overt visual surveillance is used in and around shopping malls, central business districts, bus and railway stations, auto teller machines and foyers of buildings. CCTV operates in the Queen Street Mall, Brisbane; the Cavill Mall and Orchard Avenue, Gold Coast; the Ipswich CBD; Flinders Mall, Townsville; the Cairns CBD; and the Toowoomba CBD.[505] CCTV is also used by Queensland Rail to protect property and for passenger security. Queensland Rail is progressively fitting surveillance cameras to all trains and train stations.[506]

Most recently it has been reported that Surf Life Saving Queensland is investigating the potential of high-mounted video cameras to detect swimmers in difficulty.[507]

---

500 Federal legislation impacting on surveillance within Queensland includes the *Telecommunications (Interception) Act 1979*, *Australian Federal Police Act 1979*, *Australian Security Intelligence Organisation Act 1979*, *Customs Act 1901* and the *Privacy Act 1988*.

501 Discussed in section 3.3.1 of this report.

502 Until the passing of the *Crime Commission Act* and the *Police Powers and Responsibilities Act* in November 1997, legislation only regulated law enforcement agencies' use of listening devices (prohibited by the *Invasion of Privacy Act*). The 1997 Acts refer to 'surveillance warrants' for 'surveillance devices', defined to *include* listening devices, visual surveillance devices, tracking devices and devices containing any combination of them. There have been various Queensland papers (by such bodies as the CJC, the PCJC and the Queensland Police Service Review) that have touched on police powers in relation to surveillance. The latest of these - Queensland Government (Minister for Police), *Review of Police Powers*: Discussion Paper, May 1997 - discussed a range of police powers that were subsequently included in the *Police Powers and Responsibilities Act*.

503 Introduced into the Queensland Legislative Assembly on 5 March 1998.

504 See J Swanwick, 'Cooper vows to push ahead on phone tap laws', *Courier Mail*, 19 March 1998, p 8; C Jackman, 'On tap', *Courier Mail*, 20 March 1998, p 15.

505 Australian Capital Territory. Legislative Assembly. Standing Committee on Legal Affairs of the Legislative Assembly, Report No 2, *'The Electronic Eye': Inquiry to the Efficacy of Surveillance Cameras*, September 1996, para 13.16.

506 Queensland. Legislative Assembly. Travelsafe Committee, *Inquiry into Passenger Safety and Security on the Brisbane Citytrain Network*: submission by Queensland Rail, July 1996, p 17; submission by Queensland Police Service, August 1996, p 13.

507 S Spencer, 'Beach video push gets cool reception', *Gold Coast Bulletin*, 31 March 1998, p 6.

Video surveillance is also increasingly being used in commercial premises such as banks, shops and service stations to protect property. Private retailers are the largest purchasers of video surveillance equipment in Australia.[508] In addition, employers may use visual surveillance for a range of purposes (discussed below); private investigators use covert visual surveillance for detecting insurance fraud and in other investigations; and the media use long-lens cameras to photograph newsworthy people.[509]

The use of visual surveillance in public places or in commercial premises (other than by law enforcement agencies) is currently unregulated by Queensland law.

Justifications for and arguments against surveillance

There are various justifications for, and arguments against, the uses of covert or overt surveillance. As noted above, the main argument against all forms of surveillance is that it intrudes upon privacy, in terms of privacy of the person, privacy of space or territory, privacy of communications or information privacy. (Surveillance may also involve issues of trespass to land or to property).

While the use of surveillance cameras in public and work places appears to have the public's approval, the issue of surveillance generally is of public concern.[510] There may also be a significant psychological effect of surveillance on individuals and communities.[511]

However, various justifications are proffered for the use of surveillance. In relation to its use for law enforcement purposes, surveillance is particularly effective in crime detection, especially because of its evidentiary worth at any resulting trial in court.[512] The Woods' Royal Commission into the New South Wales Police Service reported that the use of electronic surveillance was the single most important factor in achieving a breakthrough in its investigations.[513]

Apart from crime *detection*, it is also argued that surveillance is useful in crime *prevention* and public safety. However, the Standing Committee on Legal Affairs of the Legislative Assembly of the Australian Capital Territory in its Report No 2, *'The Electronic Eye': Inquiry to the Efficacy of Surveillance Cameras*, (September 1996) reported:

---

508 Privacy Committee of New South Wales, *Invisible Eyes: Report on Video Surveillance in the Workplace*, Report No 67, Privacy Committee, September 1995, p 25.

509 Privacy and the media is discussed as a discrete privacy concern in section 11.6 of this report.

510 A survey conducted by MasterCard found 44% of respondents were 'very concerned' about people videotaping their movements in public places; 25% were 'not at all concerned'. 77% of respondents were 'very concerned' about telephone bugging; 10% were 'not at all concerned': MasterCard International, *Privacy and Payments: A Study of Attitudes of the Australian Public to Privacy - Summary and Findings*, 1996, pp 11-16. Compare this, however, to findings by a Morgan Poll which found that 89% of people surveyed 'approved' of the use of surveillance cameras in public places such as shopping malls (56% 'approved strongly'; 33% 'approved mildly'). 57% of respondents approved of surveillance cameras in the work place (27% 'approved strongly'; 30% 'approved mildly'): Morgan Gallup Poll, Finding No 2969, released on the Nine Network and published in *The Bulletin*, 1 April 1997. Perhaps the apparent difference between the findings of the two studies can be reconciled by suggesting that while Australians 'approve' of using surveillance cameras in public places and in the workplace, they still express concern about the fact.

511 Although this is difficult to quantify: N Waters, 'Street surveillance and privacy', *Privacy Law and Policy Reporter*, vol 3, no 3, June 1996, p 6.

512 New South Wales Law Reform Commission, op cit, p 14.

513 Royal Commission into the New South Wales Police Service, *Final Report - Volume 2: Reform*, May 1997, p 448, cited in Simpson, op cit, p 1.

> *Despite the fact that many local government authorities have installed CCTV systems in Australia and that over 250 town centres in the United Kingdom use CCTV systems, little research exists about whether CCTV really prevents or detects crime. No substantive research has been undertaken in Australia and very few studies have been undertaken in the United Kingdom.*
>
> *The Committee considers there is an urgent need for more studies to be done, in Australia and overseas. The absence of such studies makes it extremely difficult to come to a firm view about claims that CCTV is effective in preventing or detecting crime. It is possible that public money might be wasted on wider use of CCTV without clear evidence of its effectiveness and that this public money could be used on more effective crime prevention strategies.*[514]

The New South Wales Law Reform Commission endorses the above observation and points to the argument that street surveillance may merely displace crime to areas not subject to surveillance.[515] It is also argued that as a result of street surveillance, '*marginalised and socially disadvantaged groups who already receive disproportionate attention from the criminal justice system are more likely to come to notice, standing out through unusual or stereotyped appearance or behaviour*'.[516]

On the issue of workplace surveillance, the Privacy Committee of New South Wales produced a comprehensive report in September 1995, *Invisible Eyes: Report on Video Surveillance in the Workplace* (Report No 67). The report identified that employers used workplace surveillance to monitor both staff and the public in order to protect themselves against security risks such as theft, fraud, vandalism and threats to the safety of employees.[517] However, employers might also use video surveillance to monitor the performance of employees.[518]

The New South Wales Privacy Committee's report included *Guidelines on Overt Video Surveillance in the Workplace* which prohibited:

- the use of covert video surveillance in the workplace without a permit (the issuing of a permit would require a high degree of justification);
- the use of video surveillance for monitoring individual work performance;
- the operation of video surveillance cameras in toilets, showers and change rooms; and
- the operation of video surveillance in locker rooms and employee recreation rooms without a permit.

The New South Wales Attorney-General and Minister for Industrial Relations, the Honourable J W Shaw MLC, has announced that the New South Wales government is currently

514 Australian Capital Territory. Standing Committee on Legal Affairs of the Legislative Assembly, op cit, pp 26-27. The ACT has not, as yet, introduced privacy legislation: editorial, 'Surveillance cameras on hold', *Canberra Times*, 28 December 1997, p 4.

515 New South Wales Law Reform Commission, op cit, pp 15, 33-34.

516 N Waters, June 1996, op cit, p 50.

517 Privacy Committee of New South Wales, No 67, September 1995, p 24.

518 Ibid, pp 24, 27-34.

developing legislation to implement the Privacy Committee's *Invisible Eyes* recommendations.[519]

The federal Privacy Commissioner also produced guidelines in February 1992 (*Covert Optical Surveillance in Commonwealth Administration*: *Guidelines*) for the application of the IPPs in the *Privacy Act* (Cth) to visual surveillance by Commonwealth agencies generally.

The New South Wales Law Reform Commission's Inquiry

In May 1997, the New South Wales Law Reform Commission (NSWLRC) published a comprehensive issues paper on surveillance which covers an extensive range of issues relating to surveillance under the topics of:

- what surveillance is (types of surveillance, uses of surveillance, policy issues surrounding arguments against and justifications for surveillance);
- regulation of surveillance in Australia;
- visual surveillance (overt and covert, regulation of overt visual surveillance);
- existing New South Wales legislation on covert surveillance and what it does not cover; and
- visual surveillance in the workplace.[520]

The issues paper foreshadows that the NSWLRC will produce draft legislation concerning surveillance.

11.3.2 Arguments raised in public consultation

About one quarter of the submissions received by the committee addressed the issue of surveillance. Surveillance was also addressed by some of the individual speakers at the committee's Brisbane privacy seminar and Gold Coast and Townsville public hearings. Evidence to the committee indicated that the increasing use of surveillance - in various circumstances and for various purposes - is an area of particular concern to the community.

In general, submissions recognised that the use of surveillance had the potential to significantly infringe the privacy of individuals. The Townsville Community Legal Service provided the committee with a series of disturbing 'hypotheticals' regarding the misuse of surveillance and of the information that it provides.[521] Mr J McDonald[522] attached an article reminding the committee that the International Labour Organisation has warned that the use of covert monitoring by surveillance technologies is a violation of human rights.[523]

Some submissions referred to the widespread use of surveillance. Other submissions addressed one specific use. These specific areas included law enforcement, detecting personal injury

519 Hon J W Shaw MLC, New South Wales Attorney-General and Minister for Industrial Relations, Paper presented to the Australian Privacy Summit, 21 October 1997, p 8.
520 New South Wales Law Reform Commission, op cit.
521 Townsville Community Legal Service Inc, submission dated November 1997, pp 5-7.
522 J McDonald, submission dated 17 November 1997.
523 H Gallaghur, '"1984":1997', *Australian Lawyer*, vol 32, no 8, September 1997, pp 4-5, p 4.

insurance fraud, protecting against theft in the retail industry, providing security in banks and providing security and safety in jail.

Submissions also addressed the sufficiency of regulation. Submissions either pointed to a lack of regulation concerning surveillance in Queensland (either generally or in relation to certain uses) or, in a minority of cases, argued that the use of surveillance, at least for retailing purposes, was or is becoming, sufficiently regulated by codes of practice.

The federal Privacy Commissioner stated:

> *[S]urveillance technology has advanced rapidly in recent years and uses a wide variety of means to collect information: direct visual surveillance; video recordings made using intra red, millimetre wave, visible light or other frequencies; and audio recordings using sophisticated devices. I understand that in Queensland, as in other Australian jurisdictions, the use of some of these technologies is unregulated despite their fundamentally intrusive nature. There are major inconsistencies in the treatment of different technologies, with listening devices laws applying strict controls for some forms of audio surveillance, with most video recording being completely unregulated. This suggests that some policy action in relation to this sort of activity would be desirable.*[524]

The Queensland Council for Civil Liberties highlighted what it believes to be inadequate regulation:

> *With the increased use of surveillance, in particular video surveillance both in public and private places, it is clear that there is a pressing need for regulation. Video cameras are becoming increasingly pervasive both in shopping malls, shops and public areas, with little public reaction due to the perception (by members of the public) of an increase in the level of public safety, although there is a* ***paucity of evidence to support the argument that such cameras assist in crime prevention and detection****.*
>
> *It is clear that without regulation, the use of video camera surveillance is open to significant abuse. For example, in recent times in Queensland we have seen examples of the misuse of cameras by security personnel in a major department store in order to look into women's change rooms, and to spy on women's breasts and buttocks.*
>
> *In Victoria, school authorities mounted video cameras in school washrooms in order to confirm reports of heroin use. The use of such cameras constitutes an extraordinary breach of the right to privacy which, in QCCL's view, attaches to all members of society…*[525][Emphasis added.]

While the QCCL pointed to this 'paucity of evidence' to support the purported crime prevention and detection benefits of video surveillance in public places, the CJC submitted:

> *The CJC does not oppose the use of visual surveillance cameras to enable surveillance of areas occupied by significant numbers of the public, for example the City Mall. When visiting those public places, there is, in any event, a reasonable expectation of being seen by others.*

---

524 Federal Privacy Commissioner, submission dated 28 August 1997, p 15.

525 Queensland Council for Civil Liberties, submission op cit, pp 12-13. The QCCL expanded its views on the matter at the committee's Brisbane public seminar on 17 November 1997.

> *Further, the tapes from cameras recording activities in the public space provide useful information in relation to offences and allegations against police, although there should be a restriction on those tapes being made available to the general public or the media.*[526]

However, on the issue of surveillance used for law enforcement, the CJC recognised that such surveillance should only occur after judicial consent in the form of a warrant. The CJC also noted the need to ensure that the product of surveillance methods, was not disseminated unnecessarily and that serious penalties for such improper dissemination were probably required.[527]

The Police Minister's recent discussion paper on police powers (which led to the enactment of the *Police Powers and Responsibilities Act*) also drew comment. P Henderson had concerns that an increase in police powers could enable the police to hide behind privacy laws which '*might prevent a citizen from detecting any law enforcement agencies' infringement or use of their coercive powers*". In this regard, P Henderson felt that there were '*presently no proper safeguards in place to superintend the tactical and strategic operational activities or the intelligence gathering data of the coercive law agencies of the State of Queensland*'.[528]

Su-King Hll submitted that increased police powers, such as 'bugging' powers were '*clearly necessary in combating crimes in our community. The issue is about balancing the rights of an individual against the public interest served by the increased ammunition against crime*'.[529]

Apart from law enforcement, submissions addressed uses of surveillance relating to:

- banks - to '*ensure that the personal safety of customers, employees and the general public is given the highest priority*';[530]
- correctional facilities - the Prisoners' Legal Service Inc submitted '*surveillance of an inmate, whether it be by a visual or listening device, should only be used where it is considered necessary for security and/or personal safety. Where such devices are used, the inmate or visitor must be made aware of the existence of the surveillance*';[531]
- surveillance in the workplace generally - the CJC recommended that '*surveillance, whether visual or listening, should be limited to where there is some suspected criminal activity or official misconduct, or where it is relevant for security purposes*';[532]
- the detection of insurance fraud - WorkCover Queensland submitted that '*the introduction of an increased regulatory instrument would greatly impede our investigations into fraudulent matters and the associated recovery of previously claimed benefits and costs. In respect to surveillance operations currently in progress, WorkCover complies with the [Privacy Commissioner's] February 1992 Guidelines.*

526 Criminal Justice Commission, submission dated 12 August 1997, p 8.
527 Ibid.
528 P Henderson, submission, op cit, p 2.
529 Su-King Hll, submission dated 8 July 1997, pp 7-8.
530 Australian Bankers' Association, submission dated 30 July 1997, p 15.
531 Prisoners' Legal Service Inc, submission dated 11 November 1997, p 7.
532 Criminal Justice Commission, submission, op cit, p 8.

Any alterations to the current position would incur costs outweighing the benefits associated with the implementation of additional regulation';[533]

- property protection - the Retailers Association of Queensland (RAQ) submitted:

> *We believe a retailer has a fundamental right to protect their property, stock and employees from theft, damage or physical attack and threat using both overt and/or covert surveillance. Within the retail industry, visual surveillance is used for the monitoring of activity within the workplace'…*
>
> *As a general rule CCTV* ***is not*** *used in change rooms, fitting rooms, toilet cubicles or any areas which may be considered to be of an intimate nature, or where shoppers would reasonably expect to have privacy. Our members are very careful to ensure all staff using a security aid are properly instructed and supervised in its use. Some members notify the customer of its intention to conduct video surveillance. A shopper who then enters a store which displays a notice implies that they accept the condition of entry. In return our members operate such cameras ethically. Retailers take responsibility to ensure that appropriate disciplinary action is taken if camera operators are found to be conducting surveillance in an inappropriate or unethical manner.* [534]

11.3.3 Analysis and conclusion

The use of any form of surveillance is privacy-intrusive and clearly the privacy threats posed by surveillance are increasing. New surveillance technologies are increasingly sophisticated and affordable, and are being applied in an expanding number of areas.

The current regulation of surveillance in Queensland is limited to restricting the use of listening devices (both in the public and private sectors) by the *Invasion of Privacy Act*. A number of Acts also regulate the use of surveillance by law enforcement bodies. With the passage of the *Police Powers and Responsibilities Act 1997*, regulation of the use of surveillance by law enforcement agencies has extended beyond the use of listening devices to video surveillance devices, tracking devices and combination of such devices. (It was noted in section 7.2 of this report that the Queensland Privacy Commissioner should be primarily responsible for monitoring Queensland's law enforcement agencies with respect to privacy issues, but that this matter be further considered and reported upon by the Queensland Privacy Commissioner as a matter of priority upon that officer's appointment.)

As suggested by the experience relating to the *Privacy Act* (Cth), the committee's proposed IPPs will regulate some forms of surveillance used by state government agencies, departments, contractors and GOCs. However, this would only be where a record of personal information is involved. The IPPs will not adequately address the intrusion imposed by surveillance on privacy *per se*.

---

533 WorkCover Queensland, submission dated 29 July 1997, pp 2-3.

534 Retailers Association of Queensland Limited, submission dated 9 July 1997, pp 1-3. At the committee's public seminar at the Gold Coast on 7 November 1997, Mr Ross Clarke of the RAQ informed the committee that the Australian Retailers Association has produced *Video Surveillance: Code of Practice (Second Draft)*. The draft code includes *Principles for Conducting Video Surveillance*, dealing with staff training, protecting the privacy of persons who are recorded, erasure of recordings, limiting disclosure of recordings, and the privacy of employees.

A Queensland Privacy Commissioner - with jurisdiction to address non-information privacy concerns (as recommended in the first part of this chapter) - will extend the capacity of the privacy regime to deal with surveillance. However, the committee realises that its proposed privacy regime will nevertheless still have only a limited scope to address all surveillance concerns. Private sector use of non-aural surveillance technologies will continue to come under no legislative control. The committee is particularly concerned about the proliferation of the use of CCTV monitoring of public places and commercial premises.

Therefore, there is potential for further regulation of surveillance in Queensland.

This regulation could be in the form of legislation, codes of conduct, some other type of agreement or prescription or combinations of these things (depending on the type and setting of the surveillance being regulated). The Commonwealth could well have to be involved in regulating some forms of surveillance, for example, online surveillance involving telephone lines would invoke federal jurisdiction.

The committee especially notes the extensive inquiry currently being undertaken into surveillance by the New South Wales Law Reform Commission. The committee believes that it would be duplicitous if this committee now took on a substantial inquiry into surveillance, before the NSWLRC publishes its report. However, at the same time, the committee believes that the adverse effects on individuals' privacy posed by the various forms of surveillance should be addressed in the short term.

Therefore, the committee believes that the Queensland Privacy Commissioner should reconsider the issue of surveillance used by both the private and public sectors in this state. This further inquiry should draw upon the consultation undertaken by, and the research and findings of, the New South Wales Law Reform Commission.

11.3.4 Recommendation

Recommendation 28 - The committee is concerned about the proliferation of the use of surveillance technology by both the public and private sectors.

Therefore, the committee recommends that the Queensland Privacy Commissioner, upon that Office's establishment, inquire into surveillance undertaken by the private and public sectors in Queensland. The Commissioner's inquiry should draw upon the consultation undertaken by, and the research and findings of, the New South Wales Law Reform Commission in relation to its current surveillance inquiry.

11.4 SMART CARDS AND ELECTRONIC COMMERCE

11.4.1 Background

A smart card is a plastic card which resembles a credit card but contains a computer chip which can give it the capacity to store and, in some cases, process data. Smart cards can either

operate as a contact card (that is, the card is 'read' by a smart card reader) or a contactless card (that is, the card is activated by radio waves when passed near a transmitter).[535]

As a result of their data storage and/or processing capabilities smart cards are being developed for a variety of applications. These include: electronic cash (known as stored value cards) for small purchases and for payment for such things as road tolls; the storage of information, such as medical records and identity details; and access to buildings and computer systems.[536] Smart cards may have single or multiple applications and lend themselves to use in the public and private sectors.

Stored value smart cards can also have different features such as being rechargeable, disposable, personalised, single or multi-currency and/or secured by personal identification numbers (PINs).[537] A number of stored value card trials have already been conducted in Australia.

The various applications of smart cards and the data bases used in smart card systems pose a variety of threats to the privacy of personal information. Each smart card application will raise its own privacy issues and the response to those privacy issues will depend on the organisation controlling the smart card system. (For example, it may be argued that government controlled systems should be subject to tighter regulation because governments compel people to provide information to it, and because governments have greater capacity to collect and match data.[538]) However, some privacy issues are generic to all smart card applications. These privacy issues include:

- the creation of a record of a person's movement and purchasing habits through their use of smart cards for purchases, ticketing, etc;
- the development of data profiles from matching transaction data collected from a range of daily activities. These profiles could be disclosed or used for purposes beyond the contemplation and knowledge of the individual concerned (especially marketing);
- the lack of anonymity - unlike cash, smart cards are not anonymous; and
- access to smart cards records by the government and others, including access to information held on a smart card but intended for an alternative application of the card.[539]

Earlier discussion in this report reveals the extent of information privacy laws which currently apply in Australia. Whilst any use of smart cards by Commonwealth government agencies will have to comply with the *Privacy Act* (Cth), there is currently no equivalent privacy legislation covering the state or local governments or the private sector. (Note, however, that the ACT's

535 Federal Privacy Commissioner, *Smart Cards: Implications for Privacy*, Information Paper Number Four, Australian Government Printing Service, Canberra, December 1995, p 9.

536 For further examples of smart card applications see the federal Privacy Commissioner's information paper: ibid, pp 17-33.

537 A Beatty and K Forrest, 'Privacy issues and emerging banking technology', paper presented at the AIC Conference on Privacy and Data Protection, Sydney, 19-20 March 1997, p 4.

538 Federal Privacy Commissioner, December 1995, op cit, pp 36-37.

539 Beatty and Forrest, op cit.

Fair Trading Act has, since 1996, made it an offence for a cash card provider to disclose details of the use of a cash card where those particulars identify or tend to identify the user.[540])

The federal Privacy Commissioner has identified a need for some form of smart card regulation. The three options in this regard are generally seen to be legislation, voluntary codes and/or a combination of both.[541] Any regulatory scheme will also have to accommodate both the current and potential range of smart card applications.

There have been a number of efforts by private industry sectors and groups to implement codes of practice with respect to the use of smart cards. These codes include the smart card industry code of conduct released by the Asia-Pacific Smart Card forum[542], best practice guidelines for the operation of stored value smart cards issued by the Smart Card Advisory Network (SCAN)[543] and the Credit Union Corporation (Australia) Limited code in relation to its Quicklink smart card. Apart from the privacy provisions contained in the Code of Banking Practice, the major banks have also adopted an Electronic Funds Transfer (EFT) Code of Conduct. The EFT Code of Conduct governs EFT transactions involving plastic cards used in conjunction with PINs, obliging banks to protect the information surrounding customers' EFT transactions.[544] Although, the EFT Code of Conduct only applies to a small number of smart card applications.[545]

However, there have been comments that these self-regulatory codes will not be effective without legislative backing (such as the national privacy legislation proposed for the private sector in the federal Attorney-General's 1996 Discussion Paper).[546]

As to what privacy principles smart card systems should incorporate, the federal Privacy Commissioner refers to three essential themes: first, the information collection system should be transparent (that is, the flows of information should be readily apparent); second, there should be limits on the collection and use of personal information; and third, the personal information that is collected should be accurate and secure.[547]

---

[540] However, 'cash card' is defined to only include cards electronically encoded with a monetary value to be used for the payment of goods and services. These provisions were inserted by the *Fair Trading (Amendment) Act 1996* (ACT).

[541] Federal Privacy Commissioner, December 1996, op cit, pp 51-55.

[542] This forum is an industry association hosted by the Australian Electrical and Electronic Manufacturers' Association, the Commonwealth Department of Industry, Science and Technology and the Warren Centre for Advanced Engineering at the University of Sydney.

[543] SCAN is comprised of government, industry, banks and privacy interest groups and meets regularly in Sydney. The SCAN guidelines have now been formally endorsed by a number of organisations: C Connolly, 'What rules for smart cards?', *Consuming Interest*, Spring 1996, pp 28-29.

[544] Privacy provisions contained in the EFT Code require card-issuers to: treat customer records 'in the strictest confidence'; prevent third person access through an electronic terminal to a customer's account; prevent electronic terminals being capable of providing any such information without the entry of the correct card and PIN; and prevent (unless under a legal duty to do so) disclosure of any information concerning the use of EFT services by a customer, except with the consent of the customer: Australian Bankers' Association, submission, dated 30 July 1997, p 6 and Annexure 4.

[545] It has been suggested that this model could be nevertheless extended to meet the additional applications of smart cards: G Tucker, 'Electronic payment systems: Some legal issues', *Law Institute Journal*, vol 71, no 1, January 1997, pp 29-33 at p 29.

[546] C Merritt, 'Govt told smartcard privacy needs legislative backing', *Australian Financial Review*, 4 April 1997, p 8. See also D Morrissey, 'Amex has smartcard, but privacy concern, *The Australian*, 30 September 1997, p 56.

[547] Federal Privacy Commissioner, December 1995, op cit, pp 51-52.

In 1995 the New South Wales Privacy Committee released a report *Smart Cards: Big Brother's Little Helpers*[548] in which it recommended a three-layered approach to addressing privacy and consumer concerns about smart cards. The approach included: state legislation implementing enforceable privacy standards with general application to both the public and private sectors; an industry code of conduct; and requirements that all smart card promoters be licensed which could be monitored by a body such as the Reserve Bank of Australia.

The New South Wales Privacy Committee also noted that the 'borderless' nature of smart cards would make it desirable that there is a measure of uniformity across the states.[549]

A national approach to smart cards is apparently being developed.

In March 1996, the Standing Committee of Officials of Consumer Affairs (SCOCA) formed a working party representing Queensland, New South Wales and the ACT to develop a national approach to smart cards (including stored value cards) and to prepare a report for the Ministerial Council on Consumer Affairs. In July 1996 the Queensland Office of Consumer Affairs also conducted (in conjunction with New South Wales and the ACT) a phone-in in a bid to canvass consumer views on, and experiences of, the various trials with smart cards.

A report was prepared on the results of that phone-in. One of the key matters in that report was the privacy of personal, financial and transactional information and recommendations included that the report be referred to the Standing Committee of Attorneys General in its consideration of relevant privacy issues relating to smart cards.

The Commonwealth's Online Council, which was established to achieve national cooperation and consistency in online issues, also has smart card developments on its agenda.[550]

Electronic Commerce

Electronic commerce is the '*use of electronic means to conduct transactions*'.[551] The development of stored value smart cards is only one aspect of electronic commerce; there are numerous other electronic payment systems and other dimensions of electronic commerce raise privacy concerns, such as Internet banking, digital payment systems (such as digital cash), portable EFTPOS machines, paperless share transactions, telephone banking and buying and selling on the Internet.

Electronic commerce is developing rapidly and raises legal and other issues that go beyond privacy considerations.[552] Nevertheless, privacy is a concern in relation to electronic commerce[553] and, while many of the privacy issues that relate to payment systems such as digital cash and Internet banking are similar to those relating to smart cards noted above,

548 Report No 66.

549 Ibid, p 55.

550 Refer to http://www.dca.gov.au/ogc/noframes/background.html

551 G Tucker, January 1997, op cit, p 29.

552 These legal issues include: whether digital cash constitutes legal tender or can be a negotiable instrument - it seems neither; the point in time at which value is passed and payment is irrevocable; who owns the property in smart cards; and the position when forgery is involved. See G Tucker, 1997, ibid and G Tucker, 'Some legal issues relating to digital cash on the Information Highway', *Journal of Law and Information Science*, vol 6, no 2, 1995, pp 46-67.

553 In a 1997 poll by *The Australian* newspaper 69% of respondents agreed that the banks cannot be trusted to ensure consumer's privacy in an online environment: 'Banks put profit before privacy', *The Australian*, 14 October 1997, p 36.

different payment systems raise different privacy concerns. The use of the Internet (for any purpose including Internet commerce) also means that marketers are able to track a consumer's movements through the WorldWide Web via 'cookies'.[554]

There have been a number of suggested responses to dealing with the privacy concerns that electronic commerce (including stored value smart cards) raise. These include:

- extending existing privacy legislation to the private sector (as suggested in chapter 10); however, some commentators have questioned the ability of the current IPPs[555] in s 14 of the *Privacy Act* (Cth) to deal adequately with the whole range of private sector electronic commerce activities;[556]

- regulating the use of electronic cash through an approach similar to that which developed the Electronic Funds Transfer Code of Conduct; [557] and

- that nothing really need be done by way of government or industry regulation because the technology will 'look after itself'. There is now an array of privacy technology[558] available to protect the *security* of personal and financial data and some commentators suggest that technology itself - spurred by competition to provide private and safe commerce - will be more effective than the law in giving people control over their personal information in electronic commerce.[559] (However, these security systems themselves raise issues such as who should control security mechanisms like encryption: the government, the private sector or the individual.[560])

The committee notes that there have also been recent Australian developments that recognise a need to provide legislative infrastructure and/or privacy and security guarantees in order for electronic commerce to flourish. These include:

- Victoria's proposed Electronic Commerce Framework Act to address electronic signatures, electronic evidence, computer crimes and mechanisms for the recognition of industry codes of conduct. Whilst the Victorian government recognises that the federal government should primarily address issues in this area, it sees state action as

---

554 A cookie is a bit of identity code that is written onto a person's hard disk when they visit certain WorldWide Web sites. When the person visits those sites, the cookie file on this computer is looked at to see if they have visited before. Cookies do not usually include information like an email or home address and only the site that placed the cookie can access it. However, marketers can, via the Internet, swap information about a consumer's preferences using the cookie file on the consumer's hard drive without the consumer knowing: Author, 'When your personal computer is no longer personal', *Computer Choice*, September-October 1997, pp 6-7.

555 The committee is not yet aware of any assessment of the February 1998 'national principles' in this regard.

556 Beatty and Forrest, op cit, pp 23-30; G Greenleaf, 'Privacy and cyberspace - an ambiguous relationship', *Privacy Law and Policy Reporter*, vol 3, no 5, August 1996, pp 88-92 and 'Privacy principles - irrelevant to cyberspace?', *Privacy Law and Policy Reporter*, vol 3, no 6, September 1996, pp 114-119.

557 G Tucker, January 1997, op cit, p 33.

558 This technology includes software which uses encryption and, in the case of digital cash, anonymous payment systems: Tucker, 1995, op cit, p 59.

559 See Patrick Quirk, address to the committee at its public hearing on Privacy in Queensland, Gold Coast, 7 November 1997, transcript, pp 6-9.

560 In March 1997, the OECD released its *Cryptography Policy Guidelines* which are designed to provide international guidance on such issues.

necessary because it believes that action must be undertaken immediately.[561]

- In March 1997 the Wallis report into the financial industry recognised the need '*to adopt appropriate internationally recognised standards for electronic commerce, including for electronic transactions over the Internet, and the recognition of electronic signatures*'.[562]

- The federal government has announced its intention to address electronic commerce issues. The National Office for the Information Economy (NOIE) (a separate entity within the Communications, Information Economy and the Arts portfolio and responsible to the Minister for Communications, the Information Economy and the Arts, Senator Richard Alston) is responsible for developing, coordinating and overviewing broad policy relating to a number of matters including the regulatory, legal and physical infrastructure environment for online services including facilitating electronic commerce.[563]

- The Commonwealth Parliament's Joint Committee of Public Accounts is also currently conducting an inquiry into the implications of expected growth in Internet commerce. Included in the terms of reference of the inquiry are 'the current frameworks for consumer protection and the protection of intellectual property'.[564]

11.4.2 Arguments raised in public consultation

Submissions to the committee canvassed various topics in relation to electronic commerce and, in particular, smart cards.

The majority of these submissions related to the application of smart cards in the private sector, although clearly there is also potential for smart cards to be used in the public sector. Main Roads and Queensland Transport submitted that the '*possibilities for smart cards are enormous*', foreshadowing one possible application: '*for example, Queensland Transport is evaluating the possibility of using smart cards as a future replacement for drivers licences in Queensland*'.[565]

The Department of Justice also recommended to the committee that an audit should be undertaken to '*establish the use or intended use of smart cards and other means of electronic commerce in the public sector (with a particular focus on health and transport*).' The department also suggested the development of portfolio specific codes of conduct and best practice guidelines, consistent with the national approach.

As for how smart cards should be regulated, by far the majority of submissions that addressed smart cards stated that any regulation of smart cards should be done on a national basis.[566]

---

561 As noted, in chapter 4, Victoria established two expert bodies to assess issues relevant to electronic commerce: the DPAC and the Electronic Business Framework Group (EBFG). The EBFG recommended that the Electronic Commerce Framework Act be introduced.

562 Financial System Inquiry (Chairman: S Wallis), *Final Report*, Australian Government Printing Service, Canberra, March 1997, p 57.

563 See the NOIE's Internet site at http://www.noie.gov.au/aboutnoi.html

564 See http://www.aph.gov.au/house/committee/jpaa/elecom/ectors.htm

565 Main Roads and Queensland Transport, submission dated 28 July 1997, p 3.

566 Amongst such submissions were those from the Royal Australian College of Medical Administrators (Queensland State Committee), Main Roads and Queensland Transport, International Commission of

(Although many of these submissions seemed to be referring to private rather than the public sector applications of smart cards.) The International Commission of Jurists summed up the sentiment of the majority of submissions on the matter by stating: '*the issues are national (if not international) in scope and...a coordinated national approach is sensible*'.[567] The Market Research Society of Australia added that '*an uncoordinated maze of state based systems seeking to address similar issues would likely be a draining influence on...resources.*'[568]

The precise form of regulation was addressed by few submissions. The Queensland Council for Civil Liberties suggested a 'second best' option if Commonwealth legislation regulating smart cards was not forthcoming:

> *Ideally smart card regulation should be by way of Commonwealth legislation given that neither the cards nor the companies which issue them are restricted to individual states and territories. However, in the absence of any Commonwealth legislation, a combination of state-based legislation together with national industry codes is the next best alternative. The failure of the Commonwealth Government to introduce federal legislation leaves the distinct possibility that different states will impose different regulatory regimes for smart cards, but this of course is the "downside" attaching to the failure of the Commonwealth Government to introduce the legislation that they promised in this particular area.*[569]

While the federal Privacy Commissioner's 1995 information paper discusses the desirability of a national approach to the issues surrounding smart cards (especially smart cards involving commerce), the federal Privacy Commissioner submitted to the committee that it is nevertheless:

> *... difficult to introduce technology specific regulation for a technology as flexible as the smart card, which is not more than a computer chip mounted in a standard plastic card. It can store and process information in as large a range of ways as the same chip in another physical context…It may, therefore, be undesirable to attempt to regulate smart card applications per se in legislation. Applying general privacy principles to the public and private sectors should suffice to deal with privacy issues arising from most smart card applications. A legislative option may be worthy of consideration in relation to particular applications, for example, e-cash or road tolling systems, as the privacy issues associated with them become clearer.*

However, some submissions queried whether further regulation of smart cards or electronic commerce was required at all. The Queensland Chamber for Commerce and Industry (QCCI) suggested that regulation of smart cards (at least of smart cards used in the financial system) was not currently necessary. The QCCI submitted that, for the time being, existing methods of privacy protection are adequate.[570]

In a similar vein, the Australian Bankers' Association drew the committee's attention to existing guidelines in relation to the privacy of electronic fund transfer (EFT) transactions (in

Jurists (Queensland Branch), Queensland Council for Civil Liberties, Market Research Society of Australia and the Australian Finance Conference.

567 International Commission of Jurists (Queensland Branch), submission dated 23 September 1997, p 4.

568 Market Research Society of Australia, submission dated 20 August 1997, p 5.

569 Queensland Council for Civil Liberties, submission, op cit, p 13.

570 Queensland Chamber of Commerce and Industry, submission dated 30 July 1997, pp 11-12.

terms of both the Code of Banking Practice and the Electronic Funds Transfer Code of Conduct).[571]

The Credit Union Services Corporation likewise pointed to the utility of existing guidelines that industry participants have already produced. (In relation to the first stored value card trial on the Gold Coast, credit unions developed a Credit Union Code of Conduct for Stored Value Cards.[572]) The Corporation '*felt that this Code worked well*' and submitted that the Corporation:

> *…believes that government should employ the 'light touch' of regulation That is, it should seek to reassure consumers that their personal information is protected and they have recourse under the law while not stifling innovation and technological improvements*.[573]

The Institute of Chartered Accountants[574] stated that it believed the codes of practice/conduct that already exist to cover EFT transactions and that terms of conditions that already exist to cover the use of credit cards and ATM cards '*could easily be extended to cover data generated by the use of smart cards*.'

However, the Australian Finance Conference (the national finance industry association) suggested that such codes, of themselves, might not be a sufficient form of regulation.

> *In principle, we agree that some legislative backing for the regulation should be adopted in preference to the adoption of Codes on a voluntary basis. We are concerned that without that backing Codes may not be sufficient to meet the test of "adequate" protection required by the European Union Directive ...* [575]

American Express stated:

> *The technology implications and potential for smart cards and electronic banking are not as yet fully understood. However it is clear that any overarching privacy guidelines or principles should be applicable to all consumer transactions. Voluntary codes may well be used to flesh out the details of various industries and products.*
>
> *However, the fundamental need is to have some* ***overarching framework*** *under which smart cards come. While some form of regulation for smart cards and stored value cards has been proposed in the Wallis Report, and elsewhere, some of the conflicting consumer concerns need to be addressed.*[576] [Emphasis added.]

On the wider issue of electronic commerce, the Redland Shire Council[577] referred to what it saw as '*obviously a national issue*'. The Royal Australian College of Medical Administrators (Queensland State Committee) thought a national approach would also '*obviate concern*

---

571 Australian Bankers' Association, submission, op cit, p 6 and Annexure 4.

572 Credit Union Services Corporation Australia (Ltd), submission dated 22 September 1997, p 10, enclosing the Credit Union Code of Conduct for Stored Value Cards as Annexure B to its submission.

573 Credit Union Services Corporation Australia (Ltd), ibid, p 10.

574 Institute of Chartered Accountants in Australia, submission dated 5 August 1997, p 5.

575 Australian Finance Conference, submission dated 1 August 1997, p 4.

576 American Express, submission dated 1 August 1997, p 10.

577 Redland Shire Council, op cit.

about state laws interfering with freedom of commerce between the States'.[578] Because the Department of Justice had already submitted that privacy regulation should not yet extend to the private sector,[579] the department likewise recommended that the regulation of smart cards and other means of electronic commerce should be via national industry-specific codes of conduct and best practice guidelines.

Associate Professor Patrick Quirk of Bond University informed the committee at its Gold Coast public hearing of an extensive array of specific threats that marketers could pose in relation to data collected through smart cards and electronic commerce.[580] Mr Quirk expressed concern that a voluntary scheme may not suffice in relation to regulating privacy with respect to smart cards and electronic commerce. However, he also warned that legislative attempts should proceed carefully: trying to do too much too quickly might create more problems than it solves and sector by sector regulation might be prudent. Mr Quirk warned the committee that, in the absence of clear leadership from the Commonwealth, the states should openly communicate with each other and avoid going down different paths of smart card or electronic commerce regulation.[581]

11.4.3 Analysis and conclusion

There is no doubt that smart cards will, in the very near future, become a part of our everyday dealings with both the public and private sectors. Given their current and potential applications, smart cards might be used when we catch public transport to work, buy lunch or make a phone call. Smart cards may also store everyday information such as medical histories and drivers licence details.

However, whilst smart cards will bring with them expected time and cost efficiencies, a number of privacy issues arise as a result of their current and potential uses. Smart cards and their supporting systems raise many issues relating to the collection, use, storage of, and access to, personal data. In particular, there is the potential for extensive amounts of information to be aggregated from smart cards and their use.

This is not to say that the committee believes that smart card technology should not be encouraged. As the submission of The Prince Charles Hospital and District Health Service reminded the committee, technology itself is privacy neutral, how the technology is used or abused is of the greatest concern. But, the committee believes that attention does need to be given to addressing the privacy issues that will arise from smart card use. The committee also believes that this is a matter which should be addressed now, at this early stage in the development of the smart card industry.

The three regulatory options most commonly raised to address privacy issues associated with smart cards are legislation, industry self regulation and/or a combination of both. Irrespective of which option is used, the federal Privacy Commissioner has identified that there is a need for any regulatory scheme to contain principles addressing the collection, use, access and storage of personal information. There is also a need for transparency in these systems.

---

578 Royal Australian College of Medical Administrators (Queensland State Committee), submission dated 12 June 1997, p 3.

579 See chapter 10 of this report.

580 Patrick Quirk, address to the committee at its public hearing on Privacy in Queensland, Gold Coast, 7 November 1997, transcript, pp 6-9.

581 Ibid.

Legislation could be either in the form of general information privacy principles (such as in the *Privacy Act*) being extended to cover smart card use, or specific 'smart card' privacy legislation.

However, the committee also believes that how the appropriateness of these regulatory options are judged will depend on whether the smart card system is being used in the public or private sector.

Consultation revealed that Queensland government departments are already considering uses for smart cards. The Department of Justice recommended that an audit be undertaken to establish the use or intended use of smart cards and other means of electronic commerce in the public sector (with a particular focus of health and transport). Any regulation could be considered in light of such an audit.

The federal Privacy Commissioner submitted to the committee that it may be undesirable to attempt to regulate smart cards applications per se and that general privacy principles applicable to both the public and private sectors should be able to deal with most of the privacy issues arising from smart card applications. The committee agrees with the Commissioner's comments.

In terms of regulating the use of smart cards by the *public sector*, the committee notes that the principles in the privacy legislation proposed by the committee for Queensland should be capable of addressing many of the privacy issues raised by smart cards applications. For example:

- IPP 1 would regulate the collection of information in a smart card system;
- IPP2 would operate to inform persons of the purpose for which their information was being collected (and would later be used) which would in turn give people information on which they could decide whether to participate in smart card systems;
- IPP 3 would require smart card system controllers to ensure that information about an individual and their use of the system is relevant, up to date and complete; and
- IPPs 10 and 11 would regulate the use and disclosure of personal information as part of smart card systems. In particular, this principle would be relevant when a smart card has more than one application.

Given that citizens can be compulsorily required to provide information to governments which might, in turn, form part of a smart card system, the committee believes that it is appropriate that legislative regulation should apply to the public sector. If it becomes apparent that the IPPs recommended by the committee in its privacy legislation will not be entirely applicable to smart cards, then there is scope for their application to be modified by way of a code of practice.[582]

In terms of regulating smart card applications in the *private sector*, the committee notes the various smart card industry codes of conduct currently in place. In chapter 10 of this report the committee canvassed the application of information privacy principles generally to the private sector. In particular, the committee canvassed the *National Principles for the Fair*

[582] The committee recommended that the IPPs could be amended by codes of practice in section 6.3 of this report.

Handling of Personal Information which were released by the federal Privacy Commissioner in February 1998. These principles could well operate as the benchmark for smart cards use in industry and commerce.

As previously discussed, the committee believes that any privacy regulation of the private sector needs to be undertaken on a national level. The same approach applies to smart card systems used in the private sector. Submissions to the committee made clear the need for national regulation of smart cards. A national approach to the issue of smart cards already been taken with the work of the SCOCA and its reference of smart cards issues to SCAG, and the issue of smart card developments is also on the agenda of the Online Council.

The committee has also noted in the background discussion to this section that various aspects of the broader area of electronic commerce raise privacy issues similar to those raised by smart cards, although the committee has not attempted to deal with the complex and varied privacy concerns in this regard. Clearly, a national approach is required to electronic commerce issues and there a number of organisations and processes in place to address these issues at the federal level. However, the committee does believe that this is an area in which the Queensland government should maintain an active interest to ensure that issues are being addressed in a timely and appropriate manner.

11.4.4 Recommendation

Recommendation 29 - The committee recognises that a number of privacy issues arise from the various existing and potential applications of smart cards and from the wider area of electronic commerce.

With respect to these issues in relation to departments and agencies covered by the Privacy Act (Qld), the committee:

- **notes that smart card systems will be required to comply with the information privacy principles in the Privacy Act (Qld); and**
- **recommends that the Queensland Privacy Commissioner conduct an audit to establish the use or intended use of smart cards and:**

  (a) provide relevant guidance as to any privacy issues arising as a result of that use; and

  (b) make recommendations as to any further regulation that might be required.

With respect to privacy issues arising as a result of smart cards and electronic commerce in the private sector, the committee reiterates that there must be national consistency in any privacy regulation and recommends that the Queensland government continue to support national moves that address these privacy issues in a timely and appropriate manner.

11.5 GENETICS

11.5.1 Background

In the introduction to this chapter the committee states that there are a number of discrete *information privacy* areas which require separate consideration. Genetic testing information is, the committee believes, one such discrete area.

Genetics is a new, rapidly developing field bringing with it many potential benefits in a number of areas including health care, medical research[583], determination of paternity[584] and identity, and law enforcement. However, the collection and use of personal genetic information as a result of genetic testing has immense and varied implications for privacy. It also has implications for other human rights and raises discrimination issues. For example: the rights of persons who do not wish to undergo genetic testing; discrimination on the basis of personal genetic information in relation to obtaining employment; and discrimination on the basis of genetic information in relation to seeking insurance cover.[585] Some fear that a genetic underclass may even result as a result of genetic discrimination.[586]

Many of these issues are emerging with advances in the Human Genome Project which is a project by scientists from around the world to identify and record the location of the estimated 100 000 human genes that make up the human genetic code. It is hoped that the code will be broken by early in the next century. The project raises both legal and ethical questions, many arising out of the potential for commercial applications of genetics.

In a comprehensive 1996 information paper published by the federal Privacy Commissioner, *The Privacy Implications of Genetic Testing,*[587] the Commissioner noted that personal *genetic* information differs from most other personal information in that:

- as genetic makeup is shared with the person's relatives, genetic information about one person also reveals information about the person's relatives;
- every cell in a person's body (except for sex cells) contains all of that person's genes which means that almost any sample can be tested for different genetic characteristics;
- it influences things that make up personal identity: height, build, skin colour, intelligence and possibly propensity for some behaviours such as alcoholism;
- a person's genetic makeup stays with them forever and cannot be changed; and

583 See L Skene, 'First international conference on DNA sampling: Human genetic research - Legal and policy aspects', *Journal of Law and Medicine*, vol 4, no 3, February 1997, pp 229-234; S Davies, 'The brave new world of biometric identification', *Privacy Law and Policy Reporter*, vol 2, no 2, March 1995, pp 30-31.

584 P Castle, 'Science solves paternity cases', *The Sunday Mail*, 16 July 1996, p 53.

585 P Kell and B Wynter, 'Failing your genetic test', *Consuming Interest*, no 70, Summer 1997, pp 12-15.

586 J Hay, 'Gene tests create a new underclass', *The Sunday Mail*, 2 March 1997, p 56.

587 Federal Privacy Commissioner, *The Privacy Implications of Genetic Testing*, Information Paper No 5, AGPS, Canberra, September 1996. The paper was produced as a result of a 1992 report by the House of Representatives Standing Committee on Industry, Science and Technology titled *Genetic Manipulation: The Threat or the Glory*. In response to that report the federal government requested the Privacy Commissioner to prepare a discussion paper on the privacy implications of genetic testing.

- through personal genetic information a person's future health can be predicted although often tests can only reveal a likelihood (as opposed to a certainty) that a person will exhibit a characteristic or condition. [588]

Genetic information shares similarities with other health information. Therefore, it has been noted that genetic information, being a subset of medical and healthcare information about an individual, is prima facie entitled to the same protections for privacy and confidentiality[589] which bind health professionals.[590] However, in many vital respects genetic information is clearly different to normal health information and therefore other considerations apply.

> *In particular, it has been proposed that genetic information should be shared, as a form of familial property, amongst family members who have a legitimate interest in genetic information that affects them.*[591] *The same thought can be seen in earlier suggestions about a "higher obligation" to members of society which may authorise, in exceptional cases, a breach of the general principle of medical confidentiality.*[592]

Professor Knoppers recognises that there might need to be privacy principles and exceptions for disclosure and access to genetic information in relation to the following classes of people.[593]

1 The person tested.

2 Family members who have a special status as third persons to an individual's genetic information because that information so directly relates to them.

3 Researchers.

4 Insurers, as insurance companies that are covering risks associated with health will have an interest in any information concerning their client's health.

5 Employers will also have an interest in the health information of their employees particularly where the employer pays employee insurance or superannuation premiums.

6 The State. The State may be said to have a number of responsibilities with respect to genetic information including preventing discrimination on the grounds of genetic characteristics but at the same time encouraging education about the human genome. It has also been suggested that governments should not oblige persons to undergo mandatory genetic testing to learn about genetic traits or disorders. Draft US

---

588 See also generally B Pridmore, 'Genetic testing: The privacy issues', *Privacy Law and Policy Reporter*, vol 3, no 5, August 1996, pp 85-87, 96.

589 Hon Justice Michael Kirby, 'Genetic privacy: Looking backwards - Looking forward', paper presented to the Fourth Privacy Issues Forum, Auckland, New Zealand, 10 July 1997, p 3.

590 However, as declared by the High Court in *Breen and Williams* (noted in section 10.2 of this report), there is no general common law right of access by an individual to their health records. A recent US court decision, *Moore v Regents of the University of California*, effectively stated that the plaintiff did not own their own bodily material that had been surgically removed (as noted by Senator Stott Despoja, Genetic Privacy and Non-Discrimination Bill, Second Reading Speech, March 1998).

591 World Health Organisation (WHO), *Guidelines on Ethical Issues in Medical Genetics and the Provision of Genetic Services*, WHO, Geneva, 1995.

592 Ibid.

593 Hon Justice M Kirby, referring to the work of Professor B Knoppers of the International Bioethics Committee of UNESCO, op cit, pp 3-4.

legislation provides that, except in the case of law enforcement, citizens should not be required to disclose genetic information in legal proceedings.

Each of these categories was addressed at least to some extent in the federal Privacy Commissioner's 1996 information paper. The following extracts from that paper explains the privacy issues which are raised in each of those categories.

1 The person tested

The Commissioner noted that where the information generated by a genetic test can affect only the subject of the test issues include:

- *the fundamental privacy principle that a person should exercise control over information about him or her suggests strongly that a person should not be compelled to undergo genetic testing;*

- *testing should be done on the basis of informed consent, which also requires that the person have good information about the handling of the information that the test will generate; and*

- *in order to be able to exercise control over his or her information a person requires access to that information.*[594]

2 Third persons

In cases where the information generated by a genetic test can affect people other than the subject of the test, the Commissioner noted that appropriate privacy protection is more difficult to determine. Issues identified by the Commissioner include:

- *where information from a genetic test could affect the decisions of genetic relatives of the test subject, should control over the information reside entirely with the test subject?*

- *in particular, if disclosure of genetic testing information could allow the prevention of serious health consequences in genetic relatives, should the test subject always be able to prevent disclosure?*

- *where genetic testing information suggests some risk to public safety, what approach should be taken to control over the information?*

- *where the testing of children or newborn babies is involved, decisions with a major impact on the test subject will often have to be taken by parents or guardians.* [595]

3 Research

Pursuant to the *Privacy Act*, the National Health and Medical Research Council (NHMRC) can, with the approval of the Commissioner, issue guidelines for the protection of privacy in the area of medical research. In June 1995 the Commissioner approved a revised version of the *Guidelines for the Protection of Privacy in the Conduct of Medical Research*. Under these guidelines medical research that may involve a Commonwealth agency breaching an IPP

[594] Federal Privacy Commissioner, September 1996, op cit, p 41.
[595] Ibid, p 42.

should not proceed until the relevant institutional ethics committee (IEC) decides 'that the public interest in the research outweighs to a substantial degree the public interest in the protection of privacy'.[596] Despite the Commissioner expressing some concerns about the processes set up in these guidelines, the Commissioner noted satisfaction with their practical operation.

Where the provision of personal information by Commonwealth agencies is not involved, then the IEC operating under general guidelines issued by the NHMRC considers genetic privacy issues raised by research.

The Commissioner concluded that whilst there is possibly a concern regarding the absence of a formal compliance mechanism, overall there is little evidence that there has been a mishandling of personal genetic information in the research field.[597]

4 Insurance

The Commissioner noted that currently genetic information is treated by insurance companies in the same manner as medical information, that is, insurance applicants must reveal relevant information from tests they have already had but are not obliged to have new tests.[598] Mention is also made of a then draft code of conduct for the life insurance industry regarding the use of genetic testing, including the handling of personal genetic information. (The Commissioner also indicated that it might well be efficacious if superannuation funds and health insurance funds also adopted codes of conduct setting out standards for the management of fund members' sensitive information, including personal genetic information.)[599]

In November 1996, the board of the Life, Investment and Superannuation Association (LSA) representing life insurance companies agreed to have its policy on genetic testing authorised as a binding code. (This requires the approval of the Australian Competition and Consumer Commission.) This policy, amongst other matters, requires insurance companies not to require genetic tests on applicants for insurance purposes; allows insurers to request existing genetic test results to be made available to the insurer for the purpose of classifying risk (only with the consent of the individual concerned); and states that companies will not use genetic testing as the basis for offering individuals insurance at lower than standard premium rates.[600]

5 The workplace

The Commissioner noted that, although there has been little use of personal genetic information by employers in Australian work places, employers may want genetic information to identify risks with an employee's health in general and risks associated with specific work environments. The Commissioner also observed:

596 Since 1992 the NHMRC has required that institutions in which medical (including genetic) research is undertaken must have a properly constituted IEC. These IECs must include non-scientists and they administer the NHMRC's guidelines and generally determine whether a research project is ethically acceptable.

597 Federal Privacy Commissioner, September 1996, op cit, p 51.

598 Ibid, p 72.

599 Ibid, pp 69-71.

600 Kell and Wynter, op cit, p 14.

> *Currently in Australia there is no regulatory mechanism applying to personal genetic information in a workplace context. Since the employer is often in a position of power relative to the employee or job applicant, unregulated use of genetic testing by employers clearly poses threats to the privacy of employees. As testing becomes cheaper and applicable to a wider range of conditions, the incentives for employers either to obtain the results of previous tests or to seek new tests for their employees will grow.*[601]

6 The State

DNA profiling can determine whether two samples come from the same person and therefore has potential application in both solving crimes and determining paternity. However, the Commissioner noted that, in the law enforcement context, maintaining a register of DNA samples or patterns raises serious privacy concerns:

> · *in practice, maintenance of a DNA databank would require the compulsory collection of blood samples from people convicted of classes of offences; this is clearly a serious intrusion on personal privacy;*
>
> · *personal genetic information, like all personal information, should be collected only when it serves a demonstrable purpose to do so; it is far from certain that the usefulness of a wide scope DNA databank, on the scale of existing fingerprint collections, would justify the accompanying intrusions into people's privacy;*
>
> · *there is a stronger case for a limited DNA databank containing samples from people in relation to whom there is solid evidence of likelihood to commit crimes where DNA identification is likely to be useful; and*
>
> · *although any DNA sample can be tested for any genetic characteristic, the principle of use for purpose requires that such a databank be used only for the purpose of identification.*[602]

The Commissioner also noted that privacy issues will have to be considered in proposals such as DNA databanks and increased police powers in relation to collecting blood samples.

The UNESCO Declaration and the Australian Genetic Privacy and Non-Discrimination Bill 1998

Various international bodies are becoming acutely aware of the moral, legal and ethical implications of genetic testing.

On 11 November 1997, the General Conference of the United Nations Educational Scientific and Cultural Organisations (UNESCO) unanimously adopted the Universal Declaration on the Human Genome and Human Rights (UDHGHR).[603] Part of the preamble to the UDHGHR states:

> *Recognizing that research on the human genome and the resulting applications open up vast prospects for progress in improving the health of individuals and of humankind as a whole, but emphasizing that such research should fully respect*

601 Federal Privacy Commissioner, September 1996, op cit, p 86.

602 Ibid, p 64.

603 The human genome essentially is the map of the human genetic code.

> *human dignity, freedom and human rights, as well as the prohibition of all forms of discrimination based on genetic characteristics.*

Articles 5(a)-(c), 6, 8 and 9 of the Declaration read as follows:

> ***Article 5****… a) Research, treatment or diagnosis affecting an individual's genome shall be undertaken only after rigorous and prior assessment of potential risks and benefits pertaining thereto and in accordance with any other requirement of national law.*
>
> *b) In all cases, the prior, free and informed consent of the person concerned shall be obtained. If the latter is not in a position to consent, consent, or authorization shall be obtained in the manner prescribed by law, guided by the person's best interest.*
>
> *c) The right of each individual to decide whether or not to be informed of the results of genetic examination and the resulting consequences should be respected.*
>
> *…*
>
> ***Article 6*** *No one shall be subjected to discrimination based on genetic characteristics that is intended to infringe or has the effect of infringing human rights, fundamental freedoms and human dignity.*
>
> ***Article 7*** *Genetic data associated with an identifiable person and stored or processed for the purposes of research or any other purpose must be held confidential in the conditions set by law.*
>
> ***Article 9*** *In order to protect human rights and fundamental freedoms, limitations to the principles of consent and confidentiality may only be prescribed by law, for compelling reasons within the bounds of public international law and the international law of human rights.*

Member States are also urged to make every effort (including where necessary the introduction of legislation or regulations) to promote the principles set forth in the Declaration, and to promote their implementation.[604]

On 11 March 1998, Senator Stott Despoja introduced a Private Member's Bill, the Genetic Privacy and Non-Discrimination Bill 1998, into the Australian Senate. The Bill addressed both the UDHGHR and issues set out in the federal Privacy Commissioner's 1996 information paper.

The Bill, amongst other things:

- provides for disclosure of an individual's genetic information only if:
  - (a) the individual has authorised in writing the disclosure (in a very specific manner - cl 9);
  - (b) the disclosure is required or authorised by or under law; or
  - (c) the person believes on reasonable grounds disclosure is necessary 'to prevent or lessen a serious and imminent threat to the life or health of a person' (cl 8).

[604] See article 22 and the resolution of the General Conference of UNESCO.

- provides persons with a right of access and amendment of their genetic records (cls 10 and 11);
- sets out requirements for the collection, storage and analysis of DNA samples (cls 12-16);
- provides a general prohibition against discrimination based on genetic information (cl 17);
- prohibits discrimination by employers by (subject to limited exceptions) prohibiting an employer from requesting, requiring or using the genetic information of an employee to restrict any right or benefit otherwise due or available for the employee or potential employee (cl 18);
- prohibits discrimination by insurers under cl 19; and
- regulates the use of genetic information for research and regulates the disclosure of genetic information for research purposes (cls 20-22).

In the federal Privacy Commissioner's 1996 information paper the Commissioner noted:

> *Many of the contexts in which personal genetic information may be collected or used are in the private sector. The issues raised in these contexts could most coherently be addressed in a comprehensive national framework for the protection of privacy. There have been a number of high level recommendations for such a framework and policy statements by the federal government have indicated sympathy with this approach.* [605]

The Genetic Privacy and Non-Discrimination Bill potentially represents that 'comprehensive national framework' for Australia.

11.5.2 Arguments raised in public consultation

Genetic testing as a distinct privacy issue was specifically addressed in some submissions to the committee. In particular, concerns were expressed about issues which may arise in the future in this area. The Queensland Nurses' Union informed the committee that the use of genetic testing and its impact was an area of particular concern to its members.[606] The Prince Charles Hospital and District Health Service stated:

> *Genetics is a growing area, genetic information should be treated as confidential health information, with the rights of privacy and not a basis for unlawful discrimination.*[607]

Dr Bob Brown of the Australian Medical Association (Queensland) said at the committee's Brisbane Seminar on 17 November 1997 that:

> *The science of genetics is rapidly developing and the implications of genetic knowledge and of testing are vast and far-reaching. It is vital that our society considers openly and in detail the implications of genetic testing, and it is the*

605 Federal Privacy Commissioner, September 1996, op cit, p 17.
606 Queensland Nurses Union, submission dated 7 August 1997, p 2.
607 Prince Charles Hospital and District Health Service, submission, dated 30 July 1997, p 11.

> *responsibility of our law-makers that the individual rights of people are respected and protected.*[608]

The federal Privacy Commissioner submitted to the committee:

> *There is little doubt that the handling of the personal information derived from genetic tests will be one of the most pressing information privacy issues of the coming years. Tests are becoming quicker and simpler and available for a wider range of more common conditions. The use of the information outside the health care context - for example, in the insurance industry or the labour market - poses a clear danger that those deemed genetically inferior will be marginalised and discriminated against…While personal genetic information has much in common with other sorts of sensitive medical information, its predictive power may require specific limits on its use and disclosure.* [609]

The Royal Australian College of Medical Administrators (Queensland State Committee) submitted:

> *This complex area [genetics] is full of future challenges. While genetic testing may provide evidence that one candidate may not have sufficient productive life to recompense the cost of training for a career, we must avoid a situation where only the totally genetically healthy are accepted for any form of employment. This is a case where informed public debate is necessary and ill advised legislation could do serious harm.*[610]

On the issue of genetic testing in the workplace, the Queensland Council for Civil Liberties submitted that it '*supports the rights of individuals to refuse to undergo testing, for instance, by employers who seek to screen job applicants.*' [611]

The Anti-Discrimination Commission (Queensland) reminded the committee that issues involving privacy in the workplace, in relation to medical records and in genetics may raise issues in the anti-discrimination jurisdiction.[612] On the issue of discrimination and how it is directly related to privacy, Dr Brown informed the committee:

> *According to the research by the British House of Commons completed in 1995,*[613] *there was a finding that genetic discrimination could happen inadvertently and should be prevented. In their view, the fundamental question was not about genetic information per se but about personal privacy.* ***If genetic information were treated as private to the patient or to the person concerned, and if there were adequate sanction for breach of privacy, there would be few problems of discrimination****. …[T]he House of Commons claimed that it was easy to envisage circumstances in which genetic information may be misused. Employers might deny employment to those people judged to be bad risks. The press might splash news of a public figure's genetic profile as a lead story. In fact, the media coverage in England of one particular individual's HIV status has already provided a depressing indication of*

608 Privacy in Queensland Seminar, Transcript, Brisbane, 17 November 1997, p 9.

609 Federal Privacy Commissioner, submission dated 26 August 1997, pp 16-17.

610 Royal Australian College of Medical Administrators (Queensland State Committee), submission dated 12 June 1997, p 4.

611 Queensland Council for Civil Liberties, submission dated 12 August 1997, p 17.

612 Anti-Discrimination Commission (Queensland), submission dated 1 August 1997, p 6.

613 United Kingdom. House of Commons. Science and Technology Committee, *Human Genetics: The Science and its Consequences*, 1995.

> *the kind of story that may ensure. The National Heritage Committee in Britain has already proposed that—*
>
> > *"Obtaining and/or publishing private information, such as medical records, without the permission of the person concerned or his or her next of kin should be a civil offence."* [Emphasis added.]

Dr Brown also said that:

> *Insurance is a concern as well. The availability of genetic information might have profound effects on the insurer as well as the insured. Knowledge of the results of a genetic test showing susceptibility to a serious illness gives an incentive to that person to take out a life insurance. To avoid adverse selection of risks, insurance companies in the UK now require the insured to give the results of any genetic tests they may have had, but do not require that any further tests be done. An adverse result from a test may increase the premium required or may make insurance unobtainable. This in turn gives an individual an incentive to avoid having a genetic test. Such avoidance may imperil the health and wellbeing of the insured and of their families.*[614]

The Prisoners' Legal Service Inc also raised issues regarding genetics within the correctional system.

> *Biometric scanning is a form of finger printing currently used in the correctional centres for visitors. The process is governed by Chapter 12, QCSC Policy and Procedures. Although it covers the process of finger scanning and the destruction of that information, it is open to change at any time. Information concerning a person's genetic make-up requires the protection of the legislation.*
>
> *All testing performed in the correctional system which requires the recording and/or use of genetic information (eg urine tests an body samples) must be safeguarded against abuse*.[615]

11.5.3 Analysis and conclusion

The use of genetic information raises complex legal and ethical issues, many of which concern individuals' privacy and confidentiality. In fact, genetic information could be considered the most complex 'record' of 'personal information' imaginable. On-going refinements in the science of genetics and new applications of genetic testing will continue to provide substantial moral and legal challenges in relation to individuals' privacy.

The committee has outlined in the background to this section the readily identifiable areas in which questions of access, disclosure and use of genetic information will have to be considered and some of the privacy issues in each of these categories. In many of these areas the question of use of genetic information also raises secondary or complementary issues of discrimination.

In terms of addressing privacy issues associated with genetic information, there may be some scope for modification of IPPs such as they appear in the *Privacy Act* (Cth) [and potentially in the Privacy Act (Qld)] so they can adequately and appropriately safeguard the privacy of personal genetic information. However, as Senator Stott Despoja's recent Private Member's

---

614 Privacy in Queensland Seminar, Transcript, Brisbane, 17 November 1997, pp 8.

615 Prisoners' Legal Service Inc, submission dated 11 November 1997, p 7.

Bill demonstrates, stand-alone legislation addressing genetic information privacy and issues directly related to genetics (such as discrimination) is another alternative.[616] The committee will follow the progress of the Genetic Privacy and Non-Discrimination Bill 1998 with keen interest.

Time and resources have not permitted the committee to conduct specific consultation or research in relation to each of the issues identified. Clearly, in order to assess all the privacy and other ramifications of the major genetic testing issues and/or the adequacy of existing privacy safeguards requires a good deal of specialisation. At least, consultation will need to take place with members of the scientific community, medical profession, anti-discrimination bodies and other persons with expertise in this area.

Further, the committee believes that due to the national dimension of many of the issues arising from the collection and use of genetic information, effective regulation of those issues may need to be addressed on a national basis. In this regard, the committee notes with interest the recent introduction of the Genetic Privacy and Non-Discrimination Bill 1998 and Senator Stott Despoja's accompanying comment that: '*there is a need for the Commonwealth to lead this debate and provide the guidelines*.'[617]

However, this is not to say that the committee believes Queensland should not take an active interest in issues associated with genetics. At least, the committee expects the Queensland Privacy Commissioner would monitor developments in the area of genetics and make any appropriate and/or necessary representations or recommendations. If no appropriate action is taken at the Commonwealth level, then the Queensland Privacy Commissioner may consider it necessary to recommend action at the state level. The possibilities in this regard could include a code of practice issued under the state privacy legislation, separate genetic privacy and discrimination legislation and/or amendments to state anti-discrimination legislation.

11.5.4 Recommendation

Recommendation 30 - The committee recommends that, given:

- **the complexity of the issues associated with genetic testing and the collection and use of personal genetic information; and**
- **the national dimension of many of those issues;**

the matter be the subject of further consultation and inquiry by the proposed Queensland Privacy Commissioner. However, this consultation and inquiry should be undertaken in light of developments at the federal level and in conjunction with relevant federal bodies.

---

616 The Bill nevertheless substantially incorporates the essence of various Information Privacy Principles.

617 Senator Stott Despoja, Genetic Privacy and Non-Discrimination Bill 1998, Second Reading Speech, Senate Hansard, 11 March 1998, p 592.

11.6 THE MEDIA AND PRIVACY

11.6.1 Background

As part of its inquiry the committee received submissions and evidence concerning privacy and the media.[618] Issues associated with media intrusions into individuals' privacy became more topical during the course of the committee's inquiry with events such as the Thredbo landslide, the circumstances surrounding the death of the Princess of Wales and investigations into the affairs of former Senator Bob Woods and Senator Mal Colston.

The committee addresses the media and privacy separately in this report for a number of reasons.

Firstly, whilst arguably the most significant way in which the media can breach privacy is by publishing or broadcasting personal information, the media in the course of their news-gathering activities, also have the ability to intrude on all other categories of privacy as outlined by the committee in chapter 2 of this report. The media may infringe an individuals':

- *territorial privacy* by entering premises in a bid to conduct an interview;
- *personal privacy* in media 'scrums'; and
- *communications privacy* by covertly taping personal and telephone conversations.

Secondly, the common theme in this report is that privacy is not an absolute right and that it must be weighed against other interests. Reconciling the right to privacy with the activities of the media is complicated given the inevitable conflict between this right and the public interest which can flow from the media exercising freedom of speech.

To a limited extent, the common law regulates the activities of the media via actions in, for example, trespass, nuisance and defamation. However, the ability to bring such common law actions depends on a number of factors such as access to the courts (in terms of both time and cost) and fulfilling the necessary elements to these actions.

A system of self-regulation of the media has also developed in Australia. The Australian Press Council (APC), established in 1976 by the print media industry, has a number of objects. These include maintaining the character of the Australian press in accordance with the highest journalistic standards and to preserve its established freedom, and to consider, investigate and deal with complaints about the conduct of the press.[619]

In so far as privacy is concerned, items 3 and 4 of the APC's Statement of Principles provide:

> *Item 3 - Readers of publications are entitled to have news and comment presented to them honestly and fairly, and with respect for the privacy and sensibilities of individuals. However, the right to privacy should not prevent publication of matters of public record or obvious or significant public interest. Rumour and unconfirmed reports, if published at all, should be identified as such.*

---

618 In this section the committee uses the term media to refer to all forms of media including print, television and radio media.

619 These objects are set out in the Australian Press Council's submission, dated 31 July 1997, p 1.

> *Item 4 - News obtained by dishonest or unfair means, or the publication of which would involve a breach of confidence, should not be published unless there is an over-riding public interest.*

A number of codes of practice have also been established by various broadcasting sectors and registered with the Australian Broadcasting Authority pursuant to s 123 of the *Broadcasting Services Act 1992* (Cth). These codes deal with a number of matters including program content and privacy. For example, article 4 of the Federation of Australian Commercial Television Stations (FACTS) code of practice, which has been endorsed by all Australian commercial television stations and registered by the Australian Broadcasting Authority, states that licensees in broadcasting news and current affairs programmes:

- must not use material relating to a person's personal or private affairs, or which invades an individual's privacy, other than where there are identifiable public interest reasons for the material to be broadcast; and

- must display sensitivity in broadcasting images of, or interviews with, bereaved relatives and survivors or witnesses of traumatic incidents.

Similarly, as already noted in chapter 10, the Commonwealth *Telecommunications Act 1997* requires bodies and associations that represent sections of the telecommunications industry to register industry codes of practice regarding a range of issues including privacy. There is also provision for, and an expectation that, the Australian Communications Authority will register many of these codes, thus making them legally-binding standards.

In a recent comprehensive research paper, *Privacy and the Media*, Chadwick and Mullaly study the self-regulation which exists in Australian media and make the following observations:

- self-regulation is fragmentary, in that protection of privacy is scattered across a number of codes and policies, each of which varies in its conception of privacy and level of complexity;

- the clauses in the codes and policies relevant to privacy are generally too brief and lack the depth need to assist in staff training;

- there is some inconsistency in the reasoning and results of adjudications by the Australian Press Council and little other information available about the decisions of other self-regulatory bodies, making it difficult to evaluate the effectiveness of self-regulation;

- it is difficult to enforce the requirement of respect for privacy after the breach of privacy has occurred. The adjudication of complaints concerning an invasion of privacy in effect repeats the invasion and most complaints procedures do not provide for fines or awards of compensation; and

- the available statistics show that the level of complaints about privacy is low compared to issues such as accuracy, bias and taste (although it does not necessarily flow that there is no problem or scope for improvement).[620]

[620] P Chadwick and J Mullaly, *Privacy and the Media*, Communications Law Centre Research Paper no 4 of 1997, Communications Law Centre, Melbourne, October 1997.

In the same paper, the authors recommend a number of measures to improve media self-regulation in so far as privacy is concerned. These include:

- better training for journalists both with respect to the relevant codes of conduct and ethical issues associated with the profession. Such training would '*foster more informed and ethical decision making and would lessen unjustifiable media invasions of privacy by the young and more experienced*';
- better liaison between media self-regulatory bodies which would aid in more consistent standards and decision-making;
- making complaints procedures more widely-known, accessible and responsive via means such as prominent advertising and toll-free telephone lines; and
- addressing issues associated with fines and compensation as current sanctions under the self-regulatory system do not provide sufficient redress for complainants.

The authors of the paper did not canvass the option of additional legislative regulation in order to address privacy intrusions by the media.

The issue of privacy and the media is currently being addressed as part of an inquiry by the Senate Select Committee on Information Technologies. The purpose of this inquiry is to:

> *…evaluate the appropriateness, effectiveness and privacy implications of the existing self-regulatory framework in relation to the information and communications industries and, in particular, the adequacy of the complaints regimes.*

The Senate committee has published some background material to its inquiry which indicates that it is not looking at regulation beyond self-regulation.

> *In view of the difficulties of devising and implementing an acceptable form of government-imposed regulation, self-regulation of information services has become the norm under Australian legislation.*
>
> …
>
> *The Committee's Chair, Senator Jeannie Ferris, has said self-regulatory codes operate best when they are clear and easy to understand. However they need to be flexible, so that they can respond to changes in community standards. The industry codes that are now being put in place are (or should be) dynamic, so they can adapt quickly and flexibly to changing circumstances.*
>
> *Industry codes need to meet the acceptable balance between the individual's legitimate expectation of privacy and the community's right to know, and between the right to expect protection from objectionable material against freedom of access to information and entertainment.*[621]

The federal Privacy Commissioner, in evidence to that committee's public hearing, pointed out that she has not particularly focused on regulation of the media because it is not within her jurisdiction.[622] However, in discussing self-regulatory control, the Commissioner noted that

---

621 See the committee's 'background to the inquiry' statement at http://aph.gov.au/senate/committees/

622 Proof copy of transcript of evidence taken by the committee, Sydney, 5 February 1998, p 42. It is interesting to note that, when introduced, the New Zealand Privacy of Information Bill 1991 did cover the

whilst the codes of ethics and standards are 'pretty good', they fall down in their implementation. In this regard the Commissioner noted that:

- Australia has several sets of codes instead of one uniform set of standards;
- many journalists are not members of the organisations which have codes and therefore they are not bound by those codes; and
- there are insufficient compliance mechanisms which are necessary to give the codes 'teeth'.[623]

As a result, the Commissioner recommended that the whole issue of self-regulation of privacy and the media needs to be reviewed, with particular attention to addressing these concerns.[624]

The Senate committee intends to report in June 1998.

11.6.2 Arguments raised in public consultation

A number of persons and organisations submitted to the committee that privacy issues in the context of the media need to be addressed. The Prisoners' Legal Service submitted that media intrusion needed to be addressed by legislation.

> *The media's role is to inform the public and the public does have a right to information. However, this right must be weighed up against the interests of individuals in preserving privacy and the interest of society in assuring the proper functioning of the criminal justice system. We believe there should be protection for prisoners from unnecessary intrusions into their personal life and maximising the confidentiality of personal data. Media attention at the trial of the accused as a right of the public to access information concerning crime in the community should not extend to throughout their sentence.*[625]

The QCCL also submitted that concerns relating to privacy which need to be addressed include the:

> *…frequent intrusions by the media into the privacy of individuals, both those who are in public life and those who are often involuntarily thrust into public life. A classic recent example were the published photographs of former Senator Bob Woods photographed in his backyard during the course of a domestic dispute with his wife.*[626]

news media. However, news media organisations and commentators argued against this 'unjustifiable intrusion on the freedom of the press. As a result 'news activities' of any 'news medium' (as defined in s 2) was exempted from the operation of the Act: T McBride, 'News media' in Longworth and McBride, op cit, pp 258-270, p 258. The privacy protection regime envisioned in the federal Attorney-General's 1996 Discussion Paper (op cit) also did not extend to privacy protection in relation to the activities of the media.

623 Ibid, p 46.

624 Ibid.

625 Prisoners' Legal Service, submission dated 11 November 1997, pp 7-8.

626 Queensland Council for Civil Liberties, submission, op cit, p 5.

At the Townsville public hearing, the TCLS also drew the committee's attention to an example of how the media can invade a person's privacy when they are suspected of a crime.[627]

The committee also received two submissions from media organisations and took evidence in relation to the media and privacy from Ms Mary Vernon, Assistant Editor of the Townsville Bulletin, at its Townsville public hearing. Common elements in these submissions were that:

- the existing common law and statutory law provide sufficient protection of personal privacy;
- media self-regulation through codes of practice and effective complaints procedures is the best way of achieving the right balance between the public's right to know, the media's interest in disseminating news, and the privacy of individuals; and
- additional legal regulation is an inappropriate response to potential media incursions on individuals' privacy particularly in view of the risk this poses to the media's role in facilitating free speech.

In addition, the Australian Press Council noted that, unlike most comparable democracies, Australia makes no express provision in the Constitution guaranteeing freedom of speech or freedom of the press (although the Council recognised recent High Court judgements from which it is clear that there is an implied freedom of political communication).

> *In the absence of such an express guarantee, and the minimal impact of the implied freedom of political communication, laws restricting free speech and the media will not therefore be subject to the same judicial scrutiny as in most comparable countries. Hence there is a need for great care in enacting new legislation in this area.*[628]

FACTS submitted that there have only been four complaints made concerning alleged breaches of privacy in broadcasts by commercial television stations in Queensland in the last four years. It also submitted:

> *FACTS supports the Federal Government's decision not to introduce privacy laws covering the private sector and its encouragement of the development of industry specific codes of practice. Industry self-regulation by national industries such as commercial television, encourages uniformity of practice and avoids the difficulties arising from differences in State based legislation and statutory disincentives to Queensland based operations.*[629]

At the committee's Townsville public hearing, Ms Mary Vernon spoke about the media and privacy, particularly from a regional media perspective. Whilst agreeing that legislative regulation of the media was not necessary due to defamation laws, codes of ethics etc., Ms Vernon added that the regional media is constrained by the 'small town' environment in which it works. This means that if the media does breach someone's privacy they are likely to face

627 Privacy in Queensland public hearing, Transcript, Townsville, 14 November 1997, p 3.
628 Australian Press Council, submission dated 31 July 1997, p 2.
629 Federation of Australian Commercial Television Stations, submission dated 31 July 1997, p 3.

that person again. Therefore, from the regional media perspective, privacy is a matter of accountability in the community.[630]

11.6.3 Analysis and conclusion

In this report the committee has only broadly canvassed issues associated with the media and privacy. However, as this outline indicates, a wide range of considerations come into play when examining the current (and future) ways in which privacy concerns as a result of the news-gathering and reporting activities of the media are, or can be further, addressed.

The committee has concerns about the effectiveness of the current system of self-regulation which seeks to regulate the conduct of the media in a number of areas including privacy. In this regard it generally agrees with the observations made by Chadwick and Mullaly and the federal Privacy Commissioner.

In particular, the committee agrees with the observations that the current system of self-regulation is limited in its effectiveness because:

- codes are not uniform within the various media sectors;
- it encompasses insufficient compliance mechanisms;
- it does not cover all who work in the media;
- the codes and complaints procedures are not well known in the community; and
- it offers limited redress to complainants.

Further, what is meant by privacy and respecting privacy is not sufficiently described or explained in the various codes and policies in place.

However, the committee also agrees with the statements by FACTS to the extent that any regulation of the media must be done on a national rather than a state-by-state basis. Given the manner in which the media operates, that is, via syndicated news in the case of the print media and networks in the case of radio and television, clearly any other approach would likely be unworkable.

This is not to say that the Queensland Privacy Commissioner should not have an active interest and role in relation to privacy issues which arise as a result of the media's activities. The committee believes that this should occur. However, it does mean that any reform to the current system would probably be better undertaken and implemented as part of a national approach.

On this basis, the committee trusts that the current inquiry by the Senate Select Committee which seeks to address many of the issues associated with the media and privacy, will produce many considered and appropriate recommendations.

630 Privacy in Queensland public hearing, Transcript, Townsville, 14 November 1997, p 25.

11.6.4 Recommendation

Recommendation 31 - The committee recognises:

- **the significant privacy issues that can arise in the context of media activity;**
- **concerns expressed regarding the current self-regulatory measures; and**
- **the desirability for any reform of the current system to be done on a national basis.**

Therefore, the committee supports moves to review the current system of self-regulation in relation to the media, particularly in so far as privacy is concerned.

PART 5

12. CHAPTER 12 - CONCLUSION

12.1 PRIVACY AND THE FUNDAMENTAL LEGISLATIVE PRINCIPLES

In this detailed report the committee has outlined the reasons why privacy, especially now in the 'information age', requires further attention. The committee has also identified the area in which privacy concerns should be addressed as a matter of priority; namely, information privacy in Queensland's public sector. As a result, the committee has recommended the establishment of a legislative framework within which these and other privacy concerns can be addressed.

This framework, to be established by Queensland privacy legislation, contains two principal elements: information privacy principles to be adhered to by Queensland's public sector and a new Parliamentary officer, the Queensland Privacy Commissioner. The Queensland Privacy Commissioner is to have a broad range of functions, some of which are specifically directed at ensuring departments' and agencies' compliance with the principles, and others which are more general in nature, such as monitoring technological trends for adverse effects on privacy, and educating the community generally about privacy.

In drafting this framework the committee has been conscious of the fact that privacy is not an absolute right. As was noted at the outset of this report, determining the level of protection that privacy should be afforded is fundamentally a question of determining an appropriate balance between competing interests. The committee believes that the scheme proposed in this report contains mechanisms conducive to ensuring that this balance is achieved.

However, the committee also recognises that in order to be truly effective this privacy framework needs to encourage agencies, organisations and individuals to be more privacy aware. In particular, the people who make and shape the policies on which our law is based and the drafters of our law need to be conscious of the potential for legislation to infringe individuals' privacy. There is already a pre-legislative measure in Queensland aimed at protecting individuals' rights and freedoms which the committee believes could be further utilised to ensure that this goal is fulfilled.

It was noted in chapter 3 that the *Legislative Standards Act 1992* (Qld) requires that legislation must have regard to the fundamental legislative principles (FLPs), which are described as the 'principles relating to legislation that underlie a parliamentary democracy based on a rule of law'.[631] These principles include requiring that legislation 'has sufficient regard to rights and liberties of individuals'.[632]

631 s 4(1).

632 s 4(2). It is important to note that compliance with the FLPs is not absolute as indicated by the phrase 'sufficient regard to'. In other words, s 4 also recognises that a balance must be achieved between competing interests.

The *Legislative Standards Act* also provides a list of examples as to whether legislation 'has sufficient regard to rights and liberties of individuals'.[633] The matters in this list include whether legislation:

- is consistent with principles of natural justice;
- does not reverse the onus of proof in criminal proceedings without adequate justification;
- provides appropriate protection against self-incrimination; and
- provides for the compulsory acquisition of property only with fair compensation.

These examples are merely that; they do not define 'rights and liberties of individuals' but they provide an important guide and ready reference source as to what rights and liberties legislation should, or might, have sufficient regard to. At present, this list of examples does not include an example relating to the privacy of individuals.

The Scrutiny of Legislation Committee is responsible for, amongst other matters, examining the application of the FLPs to particular Bills and to particular subordinate legislation. That committee clearly considers that privacy is a right encompassed by the FLPs. On a number of occasions the Scrutiny of Legislation Committee has adversely commented on legislative proposals that would effectively infringe individuals' privacy rights.[634]

Regardless of whether the committee's other recommendations are adopted, the committee believes that many advantages would flow from the *Legislative Standards Act* being amended to explicitly include an example relating to privacy. In particular, such an amendment would, the committee believes, expressly draw privacy issues to the attention of departmental officers when policy is formulated and drafters when legislation is drafted. Of course, it is at this stage where the consideration of the fundamental legislative principles is vital.

12.2 RECOMMENDATION

Recommendation 32 - The committee recommends that the Premier, as the Minister responsible for the *Legislative Standards Act 1992* (Qld), amend s 4(3) of that Act to insert an additional example of what is meant by whether legislation 'has sufficient regard to rights and liberties of individuals', in terms of:

> **"(l) does not allow for intrusion of the privacy of individuals (including information, communication, personal and territorial privacy) without adequate justification."**

633 These examples are listed in s 4(3).

634 For example, in its most recent Alert Digest (No 2 of 1998) the committee noted that a Bill seeking to amend the *Police Service Administration Act 1990* (Qld) did not require, at least in the case of information about suspected and convicted offenders and about the result of criminal proceedings, the imposition of mandatory requirements on disclosure. The committee was concerned that, both the clause in the Bill and the section that the Bill sought to amend, may adversely affect the rights of individuals to privacy. However, as the committee noted 'at present there is no privacy legislation in Queensland regulating the disclosure of such information'. As a result, in that report the Scrutiny Committee requested the Minister to consider amending this provision to place appropriate restrictions and conditions upon the disclosure of information.

REFERENCES

MONOGRAPHS

Australia. House of Representatives Standing Committee on Industry, Science and Technology, *Genetic Manipulation: The Threat or the Glory*, AGPS, Canberra, March 1992.

Australia. Parliament. House of Representatives Standing Committee on Family and Community Affairs, *Health Online: A Report on Health Information Management and Telemedicine*, AGPS, Canberra, October 1997.

Australia. Parliament House of Representatives. Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth*, AGPS, Canberra, June 1995.

Australia. Senate. Community Affairs References Committee, *Access to Medical Records*, Senate Printing Unit, Canberra, June 1997.

Australian Capital Territory. Government, '*Health Records: Privacy and Access - An ACT Government Position Paper*', Government Printer, Canberra, May 1997.

Australian Capital Territory. Legislative Assembly. Standing Committee on Legal Affairs, *The 'Electronic Eye': Inquiry to the Efficacy of Surveillance Cameras*, Report No 2, September 1996.

Australian Law Reform Commission, *Child Care for Kids*, Report No 70, AGPS, Canberra, 1994.

Australian Law Reform Commission, *The Coming of Age - New Aged Care Legislation for the Commonwealth*, Report No 72, AGPS, Canberra, 1995.

Australian Law Reform Commission, *Making Rights Count - Services for People with a Disability*, Report No 79, AGPS, Canberra, 1996.

Australian Law Reform Commission, *Privacy and Intrusions*, Discussion Paper No 13, AGPS, Canberra, 1980.

Australian Law Reform Commission, *Privacy*, Report No 22, Volumes 1 and 2, AGPS, Canberra, 1983.

Australian Law Reform Commission, *Review of the Archives Act 1983*, Draft Recommendations Paper 4, AGPS, Canberra, December 1997.

Australian Law Reform Commission (Report No 77) and Administrative Review Council (Report No 40), *Open Government: A Review of the Federal Freedom of Information Act 1982*, AGPS, Canberra, 1995.

Australian Privacy Charter Council, *Australian Privacy Charter*, December 1994.

Canada. Industry Canada and Justice Canada. Task Force on Electronic Commerce, *The Protection of Personal Information: Building Canada's Information Economy and Society* January 1998, see http://canada.justice.gc.ca

Chadwick, P and Mullaly, J, *Privacy and the Media*, Communications Law Centre Research Paper No 4 of 1997, Communications Law Centre, Sydney, 1997.

Commonwealth Government. Attorney-General's Department, Discussion Paper, *Privacy Protection in the Private Sector*, AGPS, Canberra, September 1996.

Cornwall, A, *Whose Health Records? Attitudes to Consumer Access to their Health Records and the Need for Law Reform*, Public Interest Advocacy Centre, October 1996.

Financial System Inquiry (Chairman: Stan Wallis), *Final Report*, AGPS, Canberra, March 1997.

Fitzgerald, G E, *Report of a Commission of Inquiry Pursuant to Orders in Council*, Government Printer, Brisbane, 1989.

Gaze, B and Jones, M, *Law, Liberty and Australian Democracy*, Law Book Company, Sydney, 1990.

Griffith, G, *Privacy and Data Protection Law Reform: Some Relevant Issues*, Briefing Paper No 15/96, NSW Parliamentary Library Research Service, June 1996.

Information Commissioner, *Annual Report 1995/96*, Government Printer, Brisbane, 1996.

Information Commissioner, *Annual Report 1996/97*, Government Printer, Brisbane, 1997.

Ireland, I, '*Any Change in the Law Must be for Parliament': Breen v Williams and Patient Access to Medical Records'*, Parliamentary Research Service, Research Paper No 7, 1997.

Longworth, E and McBride, T, *The Privacy Act: A Guide*, GP Publications, Wellington, New Zealand, 1994.

MasterCard International, *Privacy and Payments: A Study of the Attitudes of the Australian Public to Privacy - Summary and Findings*, Mastercard, 1996

Mullen, V, *'The Individuals' Right to Privacy: Protection of Personal Information in New South Wales*, NSW Parliamentary Library Briefing Paper, Parliamentary Library, April 1995.

New South Wales Law Reform Commission, *Issues Paper 12: Surveillance*, Law Reform Commission, Sydney, May 1997.

OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1980.

Ombudsman, Annual Report 1992/93, Government Printer, Brisbane, 1993.

Ombudsman, Annual Report 1993/94, Government Printer, Brisbane, 1994.

Price Waterhouse, *Privacy Survey 1997*, Price Waterhouse, Melbourne, 1997.

Privacy Commissioner, *Community Attitudes to Privacy*, Information Paper No 3, Human Rights and Equal Opportunity Commission, Sydney, August 1995.

Privacy Commissioner, *Covert Optical Surveillance in Commonwealth Administration: Guidelines*, Privacy Commissioner, Sydney, February 1992.

Privacy Commissioner, *Federal Privacy Handbook*, CCH Publications, Sydney.

Privacy Commissioner, *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector*, Consultation Paper, August 1997.

Privacy Commissioner, *Ninth Annual Report: The Operation of the Privacy Act, 1 July 1996-30 June 1997*, AGPS, Canberra, 1997.

Privacy Commissioner, *The Privacy Implications of Genetic Testing*, Information Paper no 5, AGPS, Canberra, September 1996.

Privacy Commissioner, *Smart Cards: Implications for Privacy*, Information Paper No 4, AGPS, Canberra, December 1995.

Privacy Committee of New South Wales, *Annual Report 1994/95*, Privacy Committee, Sydney.

Privacy Committee of New South Wales, *Invisible Eyes: Report on Video Surveillance in the Workplace*, Report No 67, Privacy Committee, September 1995.

Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers*, Report No 66, Privacy Committee, August 1995.

Queensland. Criminal Justice Commission, *Report on a Review of Police Powers in Queensland - Volume V: Electronic Surveillance and other Investigative Procedures*, Government Printer, Brisbane, October 1994.

Queensland. Electoral and Administrative Review Commission, *Report on Freedom of Information*, Government Printer, Brisbane, December 1990.

Queensland. Electoral and Administrative Review Commission, *Report on Review of Appeals from Administrative Decisions*, Government Printer, Brisbane, August 1993.

Queensland. Electoral and Administrative Review Commission, *Report on Review of Archives Legislation*, Government Printer, Brisbane, June 1992.

Queensland. Electoral and Administrative Review Commission, *Report on Review of the Preservation and Enhancement of Individuals' Rights and Freedoms*, Government Printer, Brisbane, August 1993.

Queensland. Legislative Assembly. Legal, Constitutional and Administrative Review Committee, *The Preservation and Enhancement of Individuals' Rights and Freedoms: Should Queensland Adopt a Bill of Rights?*, Issues Paper No 3, Government Printer, Brisbane, September 1997.

Queensland. Legislative Assembly. Legal, Constitutional and Administrative Review Committee, *Report on a Study Tour Relating to the Preservation and Enhancement of Individuals' Rights and Freedoms and to Privacy*, Report No 6, Government Printer, Brisbane, October 1997.

Queensland. Legislative Assembly. Parliamentary Committee for Electoral Administrative Review, *Archives Legislation*, Government Printer, Brisbane, November 1992.

Queensland. Legislative Assembly. Parliamentary Committee for Electoral Administrative Review, *Public Sector Auditing*, Government Printer, Brisbane, December 1991.

Queensland. Legislative Assembly. Parliamentary Committee for Electoral Administrative Review, *Report on Review of Appeals from Administrative Decisions*, Government Printer, Brisbane, May 1995.

Queensland. Legislative Assembly. Parliamentary Criminal Justice Committee, *Report on the Accountability of the CJC to the PCJC*, Report No 38, Government Printer, Brisbane, May 1997.

Queensland. Legislative Assembly. Parliamentary Criminal Justice Committee, *Report on the Review of the Criminal Justice Commission's Report on a Review of Police Powers in Queensland, Vol V: Electronic Surveillance and Other Investigative Procedures*, Report No 28, Government Printer, Brisbane, May 1995.

Queensland. Legislative Assembly. Parliamentary Criminal Justice Committee, *A Review of the Criminal Justice Commission's Report on Telecommunications Interception and Criminal Investigation in Queensland*, Report No 29, Government Printer, Brisbane, May 1995.

Queensland. Legislative Assembly. Travelsafe Committee, *Inquiry into Passenger Safety and Security on the Brisbane Citytrain Network*, Report No 23, Government Printer, Brisbane, December 1997.

Queensland Government. Minister for Police, *Review of Police Powers*: *Discussion Paper*, May 1997.

Queensland Law Reform Commission, *Assisted and Substituted Decisions*, Report No 49, Government Printer, Brisbane, August 1996.

Queensland Police Service Review (Chairman: Sir M Bingham), *Review of the Queensland Police Service*, Kingswood Press, Brisbane, 1996.

Queensland Privacy Committee, *Final Report of the Inaugural Privacy Committee*, Government Printer, Brisbane, May 1991.

Queensland Privacy Committee, *Sixth Annual Report of the Privacy Committee*, Government Printer, Brisbane, March 1991.

Sheridan, T A, *Report of the Strategic Review of the Queensland Audit Office*, Government Printer, Brisbane, 19 July 1997.

Simpson, R, *Listening Devices and Other Forms of Surveillance: Issues and Proposals for Reform*, NSW Parliamentary Library, Briefing Paper No 20/97, NSW Parliamentary Library, November 1997.

Tucker, G, *Information Privacy Law in Australia*, Longman Professional, Melbourne, 1992.

United Kingdom. House of Commons. Science and Technology Committee, *Human Genetics: The Science and its Consequences*, 1995.

United Kingdom. Committee on Privacy, *Report*, HMSO, 1972.

World Health Organisation, *Guidelines on Ethical Issues in Medical Genetics and the Provision of Genetic Services*, WHO, Geneva, 1995.

ARTICLES

Bennett, C J, 'Adequate data protection by the year 2000: The prospects for privacy in Canada', *International Review of Law Computers & Technology*, vol 11, no 1, 1997, pp 79-92.

Dixon, T, 'Privacy Charter sets new benchmark in privacy protection', *Privacy Law and Policy Reporter*, vol 2, no 3, April 1995, pp 41-45.

Gallaghur, H, '"1984":1997', *Australian Lawyer*, vol 32, no 8, September 1997, pp 4-5.

Greenleaf, G, 'The European Privacy Directive - Completed', *Privacy Law and Policy Reporter*, vol 2, no 5, June/July 1995, pp 81-86.

Greenleaf, G, 'European Privacy Directive and data exports', *Privacy Law and Policy Reporter*, vol. 2, no 6, August 1995, pp 105-108.

Greenleaf, G, 'Stopping surveillance: Beyond "efficiency" and the OECD', *Privacy Law and Policy Reporter*, vol. 3, no 8, December 1996, pp 148-152.

Greenleaf, G, 'Victoria's Data Protection Advisory Council', *Privacy Law and Policy Reporter*, vol. 3, no 4, July 1996, p 73.

Haines, R, 'The office and functions of New Zealand's Privacy Commissioner', *Government Information Quarterly*, vol 13, no 3, 1996, pp 255-274.

Kell, P and Wynter, B, 'Failing your genetic test', *Consuming Interest*, No 70, Summer 1997, pp 12-15.

Mason, B, 'Privacy and law enforcement in Queensland: A two-faced Big Brother?', *Themis*, vol 2, no 3, November 1997, pp 36-41.

McBride, T, 'State surveillance: the slippery slope? Recent examples of the emerging surveillance society in New Zealand', *Privacy Law and Policy Reporter*, vol 4, no 4, September 1997, pp 71-74.

Miller, S, 'Privacy and the Internet', *Australian Computer Journal*, vol 29, no 1, February 1997, pp 12-15.

Pridmore, B, 'Genetic testing: The privacy issues', *Privacy Law and Policy Reporter*, vol 3, 1996, pp 85-87.

Samuels, A, 'Privacy: Statutorily definable?', *Statute Law Review*, vol 17, no 2, 1996, pp 115-127.

Skene, L, 'First international conference on DNA sampling: Human genetic research - Legal and policy aspects', *Journal of Law and Medicine*, vol 4, no 3, February 1997, pp 229-234.

Stott Despoja, N, 'Personal and Private', *Alternative law Journal*, vol 22, no 4, August 1997, pp 165-169.

Waters, N, 'Street surveillance and privacy', *Privacy Law and Policy Reporter*, vol 3, no 3, June 1996, p6.

Yarrow, D, 'Developments in the law of privacy: Law and policy', *Queensland Lawyer*, vol 17, 1996, pp60-66.

NEWSPAPER ARTICLES

Castle, P, 'Science solves paternity cases', *The Sunday Mail*, 16 July 1996, p 53.

Hay, J, 'Gene tests create a new underclass', *The Sunday Mail*, 2 March 1997, p 56.

Hilvert, J, 'Voluntary privacy code rejected', *The Australian*, 2 September 1997, p 39.

Jackman, C, 'On tap', *Courier Mail*, 20 March 1998, p 15.

McIntosh, T, 'Privacy vital to business', *The Australian*, 15 April 1997, p 44.

Riley, J, 'Banks fear Victoria jumping gun on privacy', *The Australian*, 7 October 1997, p 33.

Spencer, S 'Beach video push gets cool reception', *Gold Coast Bulletin*, 31 March 1998, p 6.

Swanwick, J, 'Cooper vows to push ahead on phone tap laws', *Courier Mail*, 19 March 1998, p 8.

van Leeuwen, H, 'How to beat privacy fees', *Australian Financial Review*, 20 March 1998.

Woolley, S, 'Should we legislate for privacy?', *The Australian*, 5 March 1998, p 11.

'Chemists' computer link-up row', *The Courier-Mail*, Brisbane, 3 November 1997, p 5.

PAPERS

Greenleaf, G, 'The European Union's privacy directive - New orientations on its implications for Australia', paper presented to the 1997 Australian Privacy Summit, Sydney, 21-22 October 1997.

Kirby, Justice Michael, 'Genetic privacy: Looking backwards - Looking forward', paper presented at the Fourth Privacy Issues Forum, Auckland, New Zealand, 10 July 1997.

Kratchanov, D, 'Personal Information and the Protection of privacy', paper appended to the proceedings of the 1995 meeting of The Uniform Law Conference of Canada.

Perton, V, MP (Chairman of the Victorian Data Protection Advisory Council), 'A Privacy Act for Victoria?, paper presented at the Australian Institute of Administrative Law, Seminar, Melbourne, 26 February 1997.

Perton, V, MP, (Chairman of the Victorian Data Protection Advisory Council), 'A Privacy Act for Victoria?', paper presented at the Australian Institute of Administrative Law, Melbourne, 26 February 1997.

Perton, V, MP (Chairman of the Victorian Data Protection Advisory Council), 'Victorian initiatives in privacy, data protection and multimedia', paper presented at the Privacy and Data Protection Conference, Sydney, 19-20 March 1997.

Shaw, Hon J W, MLC, speech notes of a paper presented at the 1997 Australian Privacy Summit, Sydney, 21 October 1997.

Appendix A: Submissions Received

	SUBMISSION RECEIVED FROM
1.	Adoption Privacy Protection Group (Inc).
2.	The Royal Australian College of Medical Administrators
3.	J L Morgan
4.	Sr Marianne Whyte
5.	Mr Noel Barwick
6.	Girls' Grammar School, Rockhampton
7.	Credit Reference Association of Australian Limited
8.	Retailers' Association of Queensland Limited
9.	Credit Union Australia Limited
10.	Bank of Queensland Limited
11.	Su-King Hll
12.	Ms Kharla Kedgley
13.	R C Sadler
14.	CONFIDENTIAL
15.	Building Services Authority
16.	CONFIDENTIAL
17.	Gold Coast City Council
18.	Queensland Rail
19.	Department of Environment
20.	Sunshine Coast Rural Landholders Assoc Inc
21.	CONFIDENTIAL
22.	Residential Tenancies Authority
23.	Australian Direct Marketing Association
24.	The University of Queensland
25.	CONFIDENTIAL
26.	The Chiropractors and Osteopaths Board of Queensland
27.	Main Roads and Queensland Transport
28.	WorkCover Queensland
29.	Department of Justice
30.	P Henderson
31.	Logan City Council

	SUBMISSION RECEIVED FROM
32.	The Prince Charles Hospital and District Health Service
33.	Mr & Mrs R Milne
34.	CONFIDENTIAL
35.	Department of Emergency Services
36.	Australian Bankers' Association
37.	Federation of Australian Commercial Television Stations
38.	The Real Estate Institute of Queensland
39.	Australian Press Council
40.	Office of the Information Commissioner
41.	Mr Alex Bowman
42.	Electoral Commission, Queensland
43.	Australian Corporate Lawyers' Association
44.	Access Community Housing
45.	Anti-Discrimination Commission, Queensland
46.	Tenants' Union of Queensland Inc
47.	Community Housing & Information Centre Inc
48.	Insurance Council of Australia Limited
49.	American Express
50.	Chartered Secretaries
51.	CONFIDENTIAL
52.	I J Graham
53.	Rockhampton City Council
54.	CONFIDENTIAL
55.	Queensland Nurses Union
56.	Department of Training and Industrial Relations
57.	Redland Shire Council
58.	The Institute of Chartered Accountants in Australia
59.	Queensland Chamber of Commerce and Industry
60.	The Australian Privacy Charter Council
61.	Department of Families, Youth and Community Care
62.	Queensland Council for Civil Liberties
63.	Australian Finance Conference

	SUBMISSION RECEIVED FROM
64.	Criminal Justice Commission
65.	Anonymous
66.	Market Research Society of Australia - Queensland
67.	Mr Brett Mason
68.	CONFIDENTIAL
69.	Human Rights and Equal Opportunity Commission - Federal Privacy Commissioner
70.	CONFIDENTIAL
71.	G J Seeds
72.	Department of Public Works and Housing
73.	Credit Union Services Corporation
74.	International Commission of Jurists
75.	Prisoners' Legal Service Inc
76.	North Queensland Women's Legal Service and Townsville Women's Shelter
77.	Mr R Hugh
78.	Ms R Dearden
79.	Townsville Community Legal Service Inc.
80.	Independent Advocacy in the Tropics
81.	Mr J McDonald

Appendix B: The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

Part One — General

Definitions

1. For the purposes of these Guidelines:

   (a) **"data controller"** means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by the party or by an agent on its behalf;

   (b) **"personal data"** means any information relating to an identified or identifiable individual (data subject);

   (c) **"transborder flows of personal data"** means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

   (a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

   (b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

   (c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

   (a) as few as possible, and

   (b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

Part Two — Basic Principles of National Application

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:

(a) with the consent of the data subject; or

(b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction , use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and polices with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

(b) to have communicated to him, data relating to him:

(i) within a reasonable time;

(ii) at a charge, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Part Three — Basic Principles of International Application: Free Flow and Legitimate Restrictions

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, polices and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

Part Four — National Implementation

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

(a) adopt appropriate domestic legislation;

(b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;

(c) provide for reasonable means for individuals to exercise their rights;

(d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

(e) ensure that there is no unfair discrimination against data subjects.

Part Five — International Co-operation

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

(i) information exchange related to these Guidelines, and

(ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

Appendix C: The Information Privacy Principles (IPPs) contained in section 14 of the *Privacy Act 1988* (Cth)

Principle 1 - Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

   (b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2 - Solicitation of personal information from individual concerned

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

(d) if the collection of the information is authorised or required by or under law - the fact that the collection of the information is so authorised or required; and

(e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

Principle 3 - Solicitation of personal information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4 - Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5 - Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

    (a) whether the record-keeper has possession or control of any records that contain personal information; and

    (b) if the record-keeper has possession or control of a record that contains such information:

        (i) that nature of that information;

        (ii) the main purposes for which that information is used; and

        (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

    (a) the nature of the records of personal information kept by or on behalf of the record-keeper;

(b) the purpose for which each type of record is kept;

(c) the classes of individuals about whom records are kept;

(d) the period for which each type of record is kept;

(e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

(f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:

(a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

(b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6 - Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7 - Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

(a) is accurate; and

(b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

(a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

(b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8 - Record-keeper to check accuracy etc. of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9 - Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10 - Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

   (a) the individual concerned has consented to use of the information for that other purpose;

   (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

   (c) use of the information for that other purpose is required or authorised by or under law;

   (d) use of the information 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

   (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11 - Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

   (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

   (b) the individual concerned has consented to the disclosure;

   (c) the record-keeper 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 individual concerned or of another person;

   (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.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

LEGAL, CONSTITUTIONAL AND ADMINISTRATIVE REVIEW COMMITTEE

48TH PARLIAMENT
SECOND SESSION

MEETING ATTENDANCE RECORD*						
MEETING DATE	DARRYL BRISKEY	FRANK CARROLL	JUDY GAMIN	KEN MCELLIGOTT	GLEN MILLINER	FIONA SIMPSON
4 APRIL 1996	✓	✓	✓	✓	✓	✓
17 APRIL	✓	✓	✓	✓	✓	✓
29 APRIL	✓	✓	✓	✓	✓	✓
2 MAY	✓	✓	✓	✓	✓	✓
16 MAY PM	✓	✓	✓	✓		✓
16 MAY PM	✓	✓	✓	✓	✓	✓
11 JULY AM	✓	✓	✓	✓	✓	✓
11 JULY PM	✓	✓	✓	✓	✓	✓
25 JULY		✓	✓	✓	✓	✓
6 AUGUST AM	✓	✓	✓	✓	✓	✓
6 AUGUST PM	✓	✓	✓	✓	✓	✓
30 AUGUST AM	✓	✓	✓	✓	✓	✓
30 AUGUST PM	✓	✓	✓	✓	✓	✓
10 SEPTEMBER	✓	✓	✓	✓	✓	✓
8 OCTOBER	✓	✓	✓	✓	✓	✓
31 OCTOBER	✓	✓	✓	✓	✓	✓
13 NOVEMBER	✓	✓	✓	✓	✓	✓
14 NOVEMBER AM	✓	✓	✓	✓	✓	✓
14 NOVEMBER PM	✓	✓	✓	✓	✓	✓
14 NOVEMBER PM	✓	✓	✓	✓	✓	✓
28 NOVEMBER	✓	✓	✓	✓	✓	✓
5 DECEMBER	✓	✓	✓	✓	✓	✓
1997 30 JANUARY AM	✓	✓	✓	✓	✓	✓
30 JANUARY PM		✓	✓	✓	✓	✓
20 MARCH	✓	✓	✓		✓	✓
26 MARCH		✓	✓	✓	✓	✓
7 MAY	✓	✓	✓	✓	✓	✓
5 JUNE	✓	✓	✓	✓	✓	✓
10 JULY	✓	✓	✓	✓	✓	✓
21 AUGUST AM	✓	✓	✓	✓	✓	✓
21 AUGUST PM	✓		✓	✓	✓	✓
28 AUGUST	✓	✓	✓	✓	✓	✓
9 OCTOBER	✓	✓	✓	✓	✓	✓
20 OCTOBER	✓	✓	✓	✓	✓	✓
30 OCTOBER	✓	✓	✓	✓	✓	✓

MEETING ATTENDANCE RECORD*						
MEETING DATE	DARRYL BRISKEY	FRANK CARROLL	JUDY GAMIN	KEN MCELLIGOTT	GLEN MILLINER	FIONA SIMPSON
5 NOVEMBER		✓	✓		✓	✓
20 NOVEMBER	✓	✓	✓	✓	✓	✓
21 NOVEMBER	✓	✓	✓	✓	✓	✓
26 NOVEMBER	✓		✓	✓	✓	✓
23 DECEMBER	✓	✓	✓	✓	✓	✓
1998 27 JANUARY	✓	✓	✓		✓	✓
18 FEBRUARY	✓	✓	✓		✓	✓
23 FEBRUARY	✓	✓	✓	✓	✓	✓
4 MARCH	✓	✓	✓	✓		✓
5 MARCH	✓	✓	✓	✓	✓	✓
19 MARCH	✓	✓	✓	✓	✓	✓
2 APRIL	✓	✓	✓	✓		✓

**Mr Vince Lester MLA was also in attendance at the committee meeting held on 4 April 1996 and was an apology for the meeting held on 17 April 1996. With the reduction in committee membership from seven to six following the introduction of the Parliamentary Committees Legislation Amendment Act 1996, Mr Lester was discharged from further attendance on the Legal, Constitutional and Administrative Review Committee and appointed to the Parliamentary Criminal Justice Committee on 18 April 1996.*