

REVIEW
OF THE
PRIVACY AND PERSONAL
INFORMATION PROTECTION
ACT 1998

New South Wales Attorney General's Department

<u>CHAPTER 1: EXECUTIVE SUMMARY AND SUMMARY OF RECOMMENDATIONS</u>	2
Executive summary	2
Summary of recommendations	4
<u>CHAPTER 2: BACKGROUND TO INTRODUCTION OF THE ACT</u>	8
<u>CHAPTER 3: IMPLEMENTATION</u>	10
Relevant Acts	10
Regulations	10
Codes of Practice	11
Section 41 Directions	11
The Office of the Privacy Commissioner	11
Operations of the Office of the Privacy Commissioner	12
Advice	13
Types of complaint	13
Complaint outcomes	14
Internal Reviews	15
Administrative Decisions Tribunal (ADT)	15
Client Survey	15
Comment	16
Other jurisdictions	17
<u>CHAPTER 4: OBJECTIVES OF THE ACT</u>	18
Legislative statement of objectives	18
Second Reading Speech	18
<u>CHAPTER 5: STRUCTURE OF THE ACT</u>	19
<u>CHAPTER 6: THE INFORMATION PROTECTION PRINCIPLES</u>	20

Introduction	20
Collection	20
Storage	20
Access	20
Use	20
Disclosure	21
Analysis of submissions	21
Use and disclosure provisions	27
Cross-border flows of personal information	29
Additional Principles	30
Unique identifiers	30
Anonymity	30
<u>CHAPTER 7: CONSENT AND CAPACITY</u>	32
Substitute Consent	32
Implied consent	32
<u>CHAPTER 8: ENTITIES BOUND BY THE ACT</u>	34
Public Sector Agency	34
State Owned Corporations (SOCs)	34
Government contractors	36
<u>CHAPTER 9: PERSONAL INFORMATION</u>	38
Personal information defined	38
Exemptions to the definition of personal information	39
An individual who has been dead for more than 30 years.	40
Publicly available publication	41
Suitability for appointment or employment as a public sector official	41
Law enforcement exemptions	42
Should personal information held by cultural institutions be excluded from the ambit of the Act?	43
Collection of unsolicited information	45

Other categories of sensitive personal information _____	45
<u>CHAPTER 10: SPECIFIC EXEMPTIONS TO THE ACT</u> _____	46
Judicial functions and access to court records _____	46
Records managed under the <i>State Records Act 1998</i> _____	46
Freedom of Information Act exemptions _____	48
Section 23: law enforcement exemptions and section 24: exemptions for investigative agencies _____	50
Section 25 – exemption where non-compliance lawfully authorised _____	52
Section 27 – specific exemption for ICAC, Police Service, PIC and NSW Crime Commission _____	52
Application of the IPPs and exemptions to the IPPs _____	53
<u>CHAPTER 11: THE USE OF OTHER STATUTORY INSTRUMENTS TO MODIFY THE INFORMATION PROTECTION PRINCIPLES.</u> _____	55
Regulations _____	55
Privacy Codes of Practice _____	55
Section 41 Directions _____	57
Guidelines _____	59
Mass data matching _____	59
<u>CHAPTER 12: PUBLIC REGISTERS</u> _____	60
<u>CHAPTER 13: ROLE OF THE PRIVACY COMMISSIONER</u> _____	62
Functions _____	62
A ‘stand-alone’ Privacy Commissioner _____	63
<u>CHAPTER 14: COMPLAINT AND REVIEW MECHANISMS</u> _____	65
Introduction _____	65
Complaints _____	65
Administrative review _____	68
Internal review _____	68
Who can conduct internal reviews? _____	69

‘Person aggrieved’ _____	69
Time limits for internal review _____	70
Victimisation _____	70
Review in the ADT _____	70
Privacy Commissioner’s role _____	70
A time limit for applications _____	71
Original or review jurisdiction? _____	72
Remedies _____	72
<u>CHAPTER 15: MISCELLANEOUS MATTERS</u> _____	73
Privacy management plans, annual reporting requirements for agencies and personal information digests. _____	73
<u>CHAPTER 16: CONCLUSION</u> _____	74
<u>APPENDIX A:</u> Respondents to the review _____	76
<u>APPENDIX B:</u> Administrative Decisions Tribunal – Outcomes In Applications Pursuant To The Privacy And Personal Information Protection Act (As At 16 May 2005) _____	78

CHAPTER 1

EXECUTIVE SUMMARY AND SUMMARY OF RECOMMENDATIONS

EXECUTIVE SUMMARY

1.1 The *Privacy and Personal Information Protection Act 1998* (Privacy Act) established the first enforceable standards for the protection of personal information held by the public sector in NSW. It created the office of the Privacy Commissioner and gave the Commissioner powers to oversee the activities of the public sector, as well as protect the privacy of individuals generally. The Act also provided for the external review by the Administrative Decisions Tribunal of certain public sector conduct.

1.2 The NSW Attorney General's Department has conducted a statutory review of the Privacy Act in accordance with section 75 of that Act. That section requires the Act to be reviewed five years from the date of commencement in order to determine whether the policy objectives of the Act remain valid and whether the terms of the Act remain appropriate for securing those objectives. This report is the result of that review process, which involved seeking submissions from interested stakeholders and members of the public.

1.3 While there is no formal statement of objectives in the body of Act, the long title of the Privacy Act provides that it is an Act 'to provide for the protection of personal information, and for the protection of the privacy of individuals generally; to provide for the appointment of a Privacy Commissioner; to repeal the Privacy Committee Act 1975; and for other purposes.'

1.4 The second reading speech of the then Attorney General of NSW, the Hon JW Shaw, QC, MLC stated the objects of the Bill to be:

- to promote the protection of the privacy of individuals;
- to specify information protection principles that relate to the collection, use and disclosure of personal information held by public sector agencies;
- to require public sector agencies to comply with these principles;
- to provide for the making of privacy codes of practice for the purpose of protecting the privacy of individuals;
- to provide for the making of complaints about privacy related matters;
- for the review of conduct that involves the contravention of the information protection principles or privacy codes of practice; and
- to establish an office of Privacy Commissioner and confer on the Privacy Commissioner functions relating to privacy and the protection of personal information.

1.5 Almost all respondents supported the objectives of the Act, but most identified a number of areas where the way in which the Act has been drafted is causing problems in implementation. Many respondents made suggestions for reform aimed at simplifying the structure of the Act and increasing its transparency. Accordingly, this report makes some suggestions for reform aimed at producing a more transparent and accessible statute.

1.6 Some areas in which reform is suggested include:

- the structure of the Act;
- the information protection principles (IPPs), including the way they are applied and how exemptions are granted;
- the rules for access to and alteration of information held by the public sector;
- the application of the Act to government contractors and state-owned corporations;
- the availability of substitute consent;
- how personal information is defined;
- the role of the Privacy Commissioner; and
- administrative review practice and procedure.

1.7 In conclusion, although most respondents thought that the objectives of the Act remain valid, there was considerable concern about the difficulty of achieving these objectives when operating with the existing Act's regulatory complexities. Accordingly, a number of recommendations are made to improve operational efficiency and transparency in the protection of privacy in NSW.

SUMMARY OF RECOMMENDATIONS

Recommendation 1

- The Annual Reports of the Privacy Commissioner should provide a clear picture of the number and type of privacy complaints it receives in each year. The figures should enable direct comparison between years. The use of whole numbers, rather than percentages in the analysis of the Commissioner's workload is recommended.
- The Privacy Commissioner should be encouraged to use the information collected about the sources of the Commissioner's workload to inform the best allocation of resources. In particular, the relative importance of allocating resources to complaints handling compared with education and advice, should be reviewed.

Recommendation 2

The Act should be restructured, using the Health Privacy Act as a model, so that the information protection principles and exemptions are set out in a Schedule to the Act.

Recommendation 3:

The Privacy Commissioner should monitor, over a two-year period, whether the lack of protection for collection of sensitive personal information causes significant concerns for citizens, and, if warranted, make further submissions to the Attorney General's Department at the conclusion of the monitoring period.

Recommendation 4

Section 9 should be amended so that unauthorised collection from a third party is permitted where it is unreasonable or impracticable to collect the information from the individual to whom the information relates.

Recommendation 5

The Act should be amended so that if collection from third parties occurs, the collector should be obliged to take reasonable steps to ensure that the person about whom the information relates is advised of its collection (unless to do so would cause serious harm) and that the information collected is relevant.

Recommendation 6

The Privacy Commissioner should monitor the security of information collected and stored electronically and advise the Attorney General of any emerging practical problems with security that cannot be adequately accommodated by IPP 5.

Recommendation 7

The circumstances under which personal information can be used and disclosed should be the same. The use and disclosure principles in the more recent privacy statutes should be used as a model for the reformulation of the Privacy Act principles, although the use and disclosure of sensitive personal information should continue to be treated more restrictively.

Recommendation 8

The Privacy Commissioner should:

- Consider the privacy laws that exist in other jurisdictions, with a view to determining their adequacy for the purpose of regulating trans-border disclosures of personal information; and
- Advise the Attorney General (in accordance with a timetable agreed with the Attorney) in relation to the making of a suitable regulation (or code, if the ability to make codes is retained) to regulate trans-border disclosures of personal information.

Recommendation 9

Consideration should be given to incorporating IPPs regulating the use of unique identifiers and preserving the right to anonymity.

Recommendation 10

The Privacy Act should provide for both substitute and implied consent to agencies handling a person's personal information in appropriate circumstances.

Recommendation 11

The application of the Act to individual statutory office holders, entities that exist within a larger government agency and quasi-governmental bodies should be clarified by making a regulation that identifies or excludes public sector agencies to which the Act applies.

Recommendation 12

All NSW SOCs should be subject to privacy regulation, so that either:

- the NSW Privacy Act should apply to SOCs that are not covered by the Commonwealth Privacy Act; or
- their prescription under the Commonwealth Act should be facilitated.

Recommendation 13

The Act should provide a structure for binding non-government organizations that are contracted by public sector agencies to provide services that require the management

of personal information to conform to the terms of the Privacy Act, unless a privacy law equivalent to the NSW Privacy Act otherwise binds them. A regulation nominating equivalent privacy laws should be made.

Recommendation 14

Using the decision of the Court of Appeal in *Vice - Chancellor Macquarie University v FM* as a guide, the Act should be amended so that it is clear that the IPPs do not apply to personal information held in the minds of employees.

Recommendation 15

The provisions of the section 41 Direction about research (suitably updated) should be incorporated into the Act. Otherwise, a regulation with this effect should be made.

Recommendation 16

The Act should be amended to clarify that while unsolicited information is not subject to the collection principles, the other IPPs do apply.

Recommendation 17

The definition of sensitive personal information in the Act should include a person's criminal record.

Recommendation 18

A single set of rules (which take into account the existing regimes in the FOI, Privacy and LG Acts) for managing access to, and alteration of information, including personal information, held by the public sector should be developed and legislated.

Recommendation 19

- The exemptions for law enforcement and investigative functions in sections 23 and 24 should be simplified and applied in a similar manner to the like exemptions in the Health Privacy Act.
- Investigations concerning disciplinary proceedings and professional misconduct and the like should be specifically included in the exemptions.
- The section 41 directions relating to investigations and information sharing should likewise be incorporated into the exemptions in the Act. The exemptions should allow for a flow of information to and from an investigating agency and specifically permit the sharing of information by agencies for the purpose of briefing counsel and consulting other experts.

Recommendation 20

The Privacy Act should be amended so that it is clear that it cannot override the provisions of agencies own operational statutes which apply to regulate the management of personal information held by the agency.

Recommendation 21

Exemptions in existing codes and directions should be reviewed and, where necessary, included in the Act or in Regulations. Future variations to the application of the Act should be by way of regulation only. Consultation with the Privacy Commissioner prior to the making of a regulation should be explicitly provided for.

Recommendation 22

The Privacy Commissioner should be encouraged to continue to develop effective partnerships with the community and the public sector in developing strategies to better protect the privacy of individuals and adopt best practice strategies (based on the IPPs) for the protection of personal information.

Recommendation 23

Section 52 should be clarified to apply to conduct that is non-compliant with an IPP or the public register provisions.

Recommendation 24

Agencies should be able to out-source their internal review obligations to appropriately qualified agents.

Recommendation 25

The Act should:

- set out the scope of the Privacy Commissioner's role in the ADT as determined in consultation with the Commissioner and the President of the Tribunal, but primarily to assist in matters of statutory interpretation and privacy practice in NSW; and
- clarify that the Commissioner may appear in privacy matters before the ADT Appeal Panel.

Recommendation 26

Applicants should be allowed 60 days from the date of completion of an internal review to file an application for external review in the ADT.

Recommendation 27

The Act should make clear that privacy matters are heard in the ADT's review jurisdiction.

CHAPTER 2

BACKGROUND TO INTRODUCTION OF THE ACT

2.1 Since the early 1970's, NSW governments have been concerned about the best way of protecting the privacy interests of their citizens. To that end the NSW Privacy Committee was founded in 1974 and given a legislative basis the following year. The *Privacy Committee Act 1975* put NSW at the cutting edge of privacy protection in the developed world.

2.2 In 1980 the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* were published. The purpose of the Guidelines was to establish minimum standards for the manner in which personal information was collected, stored used and disclosed, in order to promote the free flow of information among the OECD member States.

2.3 Concerns about the protection of an individual's privacy were fuelled at a national level in the 1980's by the Australia Card debate. This culminated in the passage of the Commonwealth *Privacy Act* in 1988, which incorporated principles to guide the Commonwealth public sector in managing the personal information held by it. Those principles were based on international privacy standards, as set out in the 1980 OECD Guidelines. The application of the Commonwealth Act has been expanded in recent years, so that it now covers larger private sector organizations and all health service providers.

2.4 In 1992, the NSW Independent Commission Against Corruption (ICAC) investigated the unlawful trade in government information and recommended the introduction of privacy laws as a way of rebuilding public trust in government.

2.5 Private members' Bills proposing privacy protections were introduced into the NSW Parliament in 1991 and 1992. In 1994 the then Attorney General, the Hon. John Hannaford, MLC, introduced the *Privacy and Data Protection Bill*. It did not survive the defeat of the Coalition Government in 1995.

2.6 In 1995 the European Union adopted *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. The Directive added some additional principles to the OECD Guidelines, and extended obligations to both manual and computerised records. All members of the EU were required to adopt a consistent set of principles for the protection of personal information.

2.7 The Directive restricted disclosures of personal data from EU states to external jurisdictions that did not have sufficient legal protections for such data.

2.8 In 1998 the NSW government enacted the *Privacy and Personal Information Protection Act 1998*, second-generation legislation designed to protect personal information. Unlike the original *Privacy Committee Act*, the Privacy Act set enforceable standards for the collection, storage, use and disclosure of personal information held by the public sector. It commenced in stages, with the effect that public sector agencies were not bound by those standards until July 2000.

2.9 In 2002 the Act was amended to remove the rights of prisoners to obtain monetary compensation for breaches of the information protection principles set out in the Act.

2.10 The NSW privacy legislation was formulated against the background of both international and national privacy standards. The structure of privacy laws in all developed countries, including NSW, has been influenced by internationally-endorsed privacy principles. This was noted in the second reading speech for the NSW Bill: *“The purpose of the bill is to promote the protection of privacy and rights of the individual by the recognition, dissemination and enforcement of data protection principles consistent with international best-practice standards.”*¹

2.11 Most recently, the *Health Records and Information Privacy Act* (the Health Privacy Act) has been enacted in NSW. This Act provides specialist regulation of health information, a sub-set of personal information, in both the public and private sectors in NSW.

¹ The Hon JW Shaw, MLC, Attorney General at p 7598, NSW Legislative Council, Hansard, 17/9/98.

CHAPTER 3

IMPLEMENTATION

RELEVANT ACTS

3.1 The Privacy Act was assented to on 30 November 1998. The Act was commenced in stages to enable public sector agencies to meet their compliance requirements.

3.2 On 1 July 2000 the main sections of the Act commenced, including:

- the information protection principles;
- the rights to internal and external review (by the Administrative Decisions Tribunal (ADT)) under Part 5 of the Act; and
- the public register provisions in Part 6 of the Act.

3.3 The ADT could not award financial compensation for breaches of the Act until 1 July 2001.

3.4 The Health Privacy Act was enacted in 2002. Schedule 3 of the Act contained some important amendments to the Privacy Act (which address some of the concerns raised in submissions to this review), so that:

- health information is usually regulated by the Health Privacy Act, not the Privacy Act;
- sensitive personal information may be disclosed only where there is a serious *and* imminent threat to the life or health of the individual concerned or another person (*italics added*);
- there is potential for disclosure of personal information held by a NSW public sector agency to a Commonwealth agency to be better regulated:
- public sector agencies (and personnel), who, in good faith, give access to personal information pursuant to the Act are not liable for those acts; and,
- a regulation can be made setting fees for matters arising under the Privacy Act.

The Health Privacy Act commenced on 1 September 2004.

3.5 In 2002 the government enacted the *Privacy and Personal Information Protection Amendment (Prisoners) Act 2002* (Privacy (Prisoners) Act). This Act removed the rights of prisoners and their friends and families to receive monetary compensation for breaches of privacy by government agencies.

REGULATIONS

3.6 Two regulations affect the operation of the Privacy Act. The *Privacy and Personal Information Protection (Transitional) Regulation 1999* (1999 Regulation)

and the *Privacy and Personal Information Protection Regulation 2000* (2000 Regulation).²

3.7 The 1999 Regulation covers transitional arrangements for the Privacy Committee, which operated under the Privacy Committee Act 1975, and the application of the Privacy (Prisoners) Act.

3.8 The 2000 Regulation:

- exempts certain public sector agencies from the requirement to make a privacy management plan;
- exempts certain public registers from the provisions of Part 6 of the Privacy Act; and
- exempts the Councils of the Law Society and Bar Association from the Act.

CODES OF PRACTICE

3.9 Section 31 of the Act provides for the making of privacy codes of practice by the Attorney General, following consultation with the Privacy Commissioner. Codes modify the application of the IPPs or the public register provisions to a public sector agency or agencies.

3.10 Up until the making of the *Privacy Code of Practice (General) 2003*, codes were made in a variety of formats. Parliamentary Counsel drafted the 2003 code and undertook to draft all future codes to improve uniformity in the structure of codes.

SECTION 41 DIRECTIONS

3.11 Under section 41 of the Act the Privacy Commissioner, with the approval of the Attorney General, is empowered to exempt an agency or agencies from information protection principles or Codes, or modify the application of the same, where this is in the public interest.

3.12 Generally, section 41 directions have been drafted by the Privacy Commissioner, although the most recent directions have been drafted by the Crown Solicitor's Office.

3.13 A list of codes and section 41 Directions can be found on the PrivacyNSW website (via www.lawlink.nsw.gov.au).

THE OFFICE OF THE PRIVACY COMMISSIONER

3.14 The Privacy Act provides for the appointment of a Privacy Commissioner by the Attorney General, subject to such terms and conditions as the Attorney determines. The position holder is remunerated in accordance with the Statutory and Other Offices Remuneration Act 1975. The Minister may determine travelling and subsistence allowances.

² Now the *Privacy and Personal Information Protection Regulation 2005*

3.15 The Commissioner's functions are set out in the Act as being:

- a) to promote the adoption of, and monitor compliance with, the information protection principles;
- b) to prepare and publish guidelines relating to the protection of personal information and other privacy matters, and to promote the adoption of such guidelines;
- c) to initiate and recommend the making of privacy codes of practice;
- d) to provide assistance to public sector agencies in adopting and complying with the information protection principles and privacy codes of practice;
- e) to provide assistance to public sector agencies in preparing and implementing privacy management plans in accordance with section 33;
- f) to conduct research, and collect and collate information, about any matter relating to the protection of personal information and the privacy of individuals;
- g) to provide advice on matters relating to the protection of personal information and the privacy of individuals;
- h) to make public statements about any matter relating to the privacy of individuals generally;
- i) to conduct education programs, and to disseminate information, for the purpose of promoting the protection of the privacy of individuals;
- j) to prepare and publish reports and recommendations about any matter (including developments in technology) that concerns the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of individuals;
- k) to receive, investigate and conciliate complaints about privacy-related matters (including conduct to which Part 5 applies); and
- l) to conduct such inquiries, and make such investigations, into privacy-related matters as the Privacy Commissioner thinks appropriate.

3.16 The Act also establishes the Privacy Advisory Committee. Its functions are:

- a) to advise on matters relevant to the Privacy Commissioner's functions;
- b) to recommend material to the Privacy Commissioner for inclusion in guidelines to be issued by the Privacy Commissioner in exercising the Commissioner's functions; and
- c) to advise the Minister on such matters as may be referred to it by the Minister.

3.17 The activities of the Privacy Commissioner and the office are detailed in Annual Reports to Parliament. The PrivacyNSW website also provides details of the role of the Privacy Commissioner in protecting privacy in NSW.

OPERATIONS OF THE OFFICE OF THE PRIVACY COMMISSIONER

3.18 The annual reports of the Privacy Commissioner for the reporting years 1999-2000, 2000-01, 2001-02, and 2002-03 have been analysed for the purposes of this review.

3.19 From 1 June 1999 the Privacy Commissioner began to exercise the powers to investigate complaints, to advise on compliance with the Act and to recommend the making of privacy codes of practice. The reported activities of the Privacy Commissioner reflect this staged commencement of the Act.

Advice

3.20 One of the Commissioner's functions is to provide advice about the protection of personal information and the privacy of individuals.

3.21 The Commissioner's Annual Reports reveal that NSW public sector agencies asked for advice about their privacy obligations more frequently than any other organisational sector. Local government was the section of the public sector that sought most assistance.

3.22 While it is apparent that the majority of advices provided by the Commissioner covered all the information protection principles, the principles of most concern were those concerning collection of personal information and its disclosure to third parties. In the reporting year ended 30 June 2003 the principle regulating use emerged as a new and growing area of concern.

3.23 The way in which the statistics concerning the Privacy Commissioner's advice case load are reported make it difficult to determine the number of advices actually provided in a given year. For instance, the 1999-2000 Annual Report does not report advice requests, but it does report that 168 advice files were closed in that year. By the 2002-2003 reporting year files opened and closed were reported.³ However, even with the figures provided it is not possible to conclude with certainty how many advices were actually given in that year.⁴

Types of complaint

3.24 Complaints about breaches of privacy range across the whole gambit of privacy concerns, including neighbourhood disputes and actions of private sector organizations, as well as the actions of NSW government agencies. When investigating complaints that cannot be dealt with by the Privacy Act (or the Health Privacy Act) or by reference to other privacy-related laws, the Commissioner applies NSW's Data Protection Principles.⁵

³ The 2002-2003 Annual Report (at page 13) reports that 218 advice files were opened and 230 closed.

⁴ For instance, some of the 230 files closed could have included some of the 218 opened. Also, the figures do not reflect the extent of the advice given.

⁵ Privacy NSW has formally adopted the data protection principles (DPPs) developed by the New South Wales Privacy Committee in 1991. The full text of the data protection principles is available on the PrivacyNSW website. The data protection principles have a more general application and are not subject to the exemptions which apply to the information protection principles under the Privacy Act.

3.25 While there is a rising trend in complaints involving the NSW public sector the actual numbers of complaints are low, rising from 36 (covering both state and Commonwealth public sectors) in 1999-2000⁶ to about 100 in 2002-2003.⁷

3.26 Complaints about the public sector do have some common features. Disclosure of personal information dominates, followed by complaints about the collection of personal information. In all but the last reporting year the most common categories of information or practice at issue in the public sector complaints were health records, criminal records and personal contact details. In 2002-2003 health records continued to be the biggest area of concern, followed by surveillance/physical privacy, identity records and investigation/law enforcement practices.

3.27 The health, education, justice and local government sectors of the public service were most likely to be the respondent in public sector complaints. Complainants were usually the clients, customers or patients of the agency, followed by agency employees (peaking at 27% in 2000-2001 before falling to 12% of complaints in 2001-2002).

3.28 Private sector complaints have focused on areas such as surveillance, debt collection, real estate/tenancy issues; the behaviour of insurance companies, not-for-profit organizations, and financial institutions; and neighbourhood disputes.

Complaint outcomes

3.29 In 1999-2000 conciliation was the dominant method for resolving complaints. In each subsequent year the number resolved in this way dropped, while referrals to internal review increased. In December 2001 the Commonwealth Privacy Act provisions governing the conduct of many private sector organizations commenced. The commencement of these provisions meant that many complaints about the conduct of private sector organizations previously dealt with by the NSW Privacy Commissioner could now be referred to the Commonwealth Privacy Commissioner for investigation and conciliation. In 2001-2002 26% of all complaints were forwarded to another complaints body, predominately the Commonwealth Privacy Commissioner, pursuant to the new Commonwealth jurisdiction.

3.30 There were two special reports to Parliament in 2001-2002, one concerning the investigation of a complaint by a local government councillor relating to a disclosure by Queanbeyan City Council and its General Manager. The second concerned a complaint made by Student A and his family against the then Minister for Education.

3.31 Of the 40 matters (out of 221 finalised complaints) that proceeded to conciliation and/or investigation in 2002-2003, a violation or interference in privacy

⁶ This figure is not actually reported. It has been calculated by reference in the 2000-2001 Annual Report (at page 14) to the fact that complaints about State and Commonwealth (governments) in the previous (1999-2000) year made up 15.8% of the total number of complaints, which was reported in the 1999-2000 Annual Report to be 227 (at page 12) – hence the calculation: $227 \times 15.8\% = 35.87$.

⁷ The actual figure is not reported. The 2002-2003 Annual Report (at page 21) states that 180 new complaints were received and 221 finalised. Of the finalised complaints, $\frac{1}{2}$ (110) concerned public sector agencies (state or local).

was found in only five cases. 20 matters were resolved without a formal finding. In four cases the matter could not be resolved and in 11 cases a finding of no privacy violation was made. 40% were referred to another complaints body⁸ and 24% were referred to internal review.⁹

INTERNAL REVIEWS

3.32 From July 2000 public sector agencies could be requested to conduct internal reviews in relation to privacy complaints. Agencies are required to notify Privacy NSW of an application for internal review and keep it informed as to the progress and outcome of the application.

3.33 The number of internal reviews notified to Privacy NSW has increased from 31 in 2000-2001 to 108 in 2002-2003. Usually the applicant is a client, customer, or patient of the agency. The second most likely applicant is an employee of the agency.

3.34 The most common types of complaint related to health records and personal contact details, with complaints about investigation and law enforcement records; client/customer records and identity records becoming more prominent in 2002-2003.

3.35 The most common information protection principle in issue was disclosure of personal information to third parties, followed by collection of personal information and use.

3.36 In 2002-2003 65 internal reviews were completed. A breach of the IPPs was found by the agency in 18 cases (28%). Multiple remedies were frequently offered, including apologies (13 cases), rectification (seven cases) and financial compensation (two cases). Changes to agency practice were promised in seven cases and retraining of staff in 10 cases.

ADMINISTRATIVE DECISIONS TRIBUNAL (ADT)

3.37 Since the ADT's jurisdiction commenced¹⁰ a total of 91 Privacy Act applications have been disposed of. The vast majority of applications have been dismissed (following settlement, withdrawal or because the Tribunal did not have jurisdiction). Only seven applications have resulted in a finding that the agency contravened the Privacy Act. In six of those cases the Tribunal took no action. Only one matter has resulted in the respondent's decision being set aside. A full analysis of the ADT statistics relating to its privacy jurisdiction is at Appendix B.

CLIENT SURVEY

⁸ As the impact of the broader jurisdiction of the Commonwealth Privacy Commissioner continued to be felt.

⁹ An increasing percentage, as the impact of the requirement that the conduct have occurred since 1 July 2000 decreases.

¹⁰ The Tribunal can review the conduct of public sector agencies which occurred after 1 July 2000.

3.38 In 2001-2002 a client satisfaction survey was conducted as part of an independent resourcing review of Privacy NSW (the Andersen Report).

3.39 The survey found that, generally speaking, clients (both agencies seeking advice or complainants seeking dispute resolution) were satisfied with the quality of Privacy NSW's work, but not its timeliness.

3.40 The survey highlighted a significant unmet demand for ongoing education and training of public sector agencies and better communication with stakeholders. In addition there was inadequate resourcing to meet the demands on core complaints, advice, and internal review work.

3.41 Overall the report found there was a reactive, rather than proactive approach to privacy management.

3.42 The Privacy Commissioner advises that subsequent to the report, some additional staff were recruited to the Office.

COMMENT

3.43 One of the primary objectives of the Privacy Act is that NSW public sector agencies will comply with the information protection principles.

3.44 As at June 2003 there were 344,000 employees in the public sector, nearly 72% of whom are employed in the health, education and public order and safety sectors.

3.45 When comparing the size and make up of the public sector with the actual numbers of complaints handled by the Privacy Commissioner or the subject of an adverse determination in the ADT, it is possible to conclude that privacy protections set out in the Privacy Act are reasonably effective in protecting patients, clients, or customers from abuses of their personal information by the public sector.

3.46 In the context of a large public sector, the relatively small numbers of complaints to the Commissioner and applications to the ADT and the even smaller numbers of adverse findings that result from them, are significant.

3.47 Because the Privacy Commissioner's Annual Reports analyse contact with the public and government agencies about privacy matters using percentages, rather than actual numbers of matters; and because the types of contact reported on have varied over time, it is difficult to get an accurate picture of the work of the Commissioner's Office or of emerging trends.

3.48 An analysis of the available statistics suggest that the limited resources of the Privacy Commissioner may be best spent in supporting the public sector, by education and advice about privacy and the application of the information protection principles, rather than in maintaining a large complaints-based practice.

The Annual Reports of the Privacy Commissioner should provide a clear picture of the number and type of privacy complaints it receives in each year. The figures should enable direct comparison between years. The use of whole numbers, rather than percentages in the analysis of the Commissioner's workload is recommended.

The Privacy Commissioner should be encouraged to use the information collected about the sources of the Commissioner's workload to inform the best allocation of resources. In particular, the relative importance of allocating resources to complaints handling compared with education and advice, should be reviewed.

OTHER JURISDICTIONS

3.49 Subsequent to the NSW Privacy Act, legislation has been passed in other jurisdictions:

- amending the Commonwealth Privacy Act to create national privacy principles for the private sector;
- creating information privacy (for the public sector) and health privacy (for the public and private sector) laws for Victoria; and
- creating information privacy laws for the Northern Territory public sector.

3.50 This review was conducted against the background of a Senate Legal and Constitutional Committee inquiry into the Commonwealth Privacy Act; a review of the private sector provisions of the Commonwealth Privacy Act by the Commonwealth Privacy Commissioner;¹¹ and a review of the Victorian Information Privacy Act. The Commonwealth is also reviewing the laws relating to privacy of employee records. Tasmania is expected to enact privacy laws shortly.

3.51 In NSW, the Parliamentary Committee on the Office of the Ombudsman and the Police Integrity Commission has delayed consideration of whether to proceed further with its Inquiry into Access to Information, pending the completion of this review.

¹¹ The report of that review by the Office of the Privacy Commissioner, "*Getting in on the Act: The Review of the Privacy Sector Provisions of the Privacy Act 1988*" was released in May 2005.

CHAPTER 4

OBJECTIVES OF THE ACT

LEGISLATIVE STATEMENT OF OBJECTIVES

4.1 The long title of the Privacy Act provides that it is an Act ‘to provide for the protection of personal information, and for the protection of the privacy of individuals generally; to provide for the appointment of a Privacy Commissioner; to repeal the Privacy Committee Act 1975; and for other purposes.’

4.2 There is no formal statement of objectives in the body of Act.

SECOND READING SPEECH

4.3 In order to understand the objectives of the Act it is necessary to go to the second reading speech of the then Attorney General of NSW, the Hon JW Shaw, QC, MLC.

4.4 The second reading speech states the objects of the Bill to be:

- to promote the protection of the privacy of individuals;
- to specify information protection principles that relate to the collection, use and disclosure of personal information held by public sector agencies;
- to require public sector agencies to comply with these principles;
- to provide for the making of privacy codes of practice for the purpose of protecting the privacy of individuals;
- to provide for the making of complaints about privacy related matters;
- for the review of conduct that involves the contravention of the information protection principles or privacy codes of practice; and
- to establish an office of Privacy Commissioner and confer on the Privacy Commissioner functions relating to privacy and the protection of personal information.

4.5 Although many of the submissions expressed dissatisfaction with operation of the terms of the Act, there was widespread agreement amongst public sector respondents that, nonetheless, it was meeting its objectives.

CHAPTER 5

STRUCTURE OF THE ACT

5.1 The information protection principles (IPPs) set out in Part 2 of the Act form the backbone of the protection of personal information held by the public sector in NSW. They are a set of legal rules about how personal information is to be collected, stored, used and disclosed by the NSW public sector.

5.2 It is clear from submissions to this review that public sector agencies have concerns about the practical difficulties in applying the IPPs and exemptions to them. The concerns expressed range from the simple to the complex.

5.3 For instance, the practice of referring to the principles as IPPs 1-12 rather than sections 8-19 is cited by a number of respondents as being confusing and unhelpful.

5.4 The fact that exemptions to these principles are scattered throughout the Act (including within the principles themselves), as well as being found in the Regulations, codes and section 41 directions was a subject of common frustration amongst respondents.

5.5 Some respondents suggested that the structure of the Act gives an illusion of privacy protection that is not sustainable on closer examination of its exemption provisions.

5.6 A number of respondents cite the structure of the recently commenced Health Privacy Act, which sets out the information protection principles applicable to health information as a schedule to the Act and follows each principle with the relevant exemptions, as being clearer and more accessible than the structure of the comparable Privacy Act provisions.

Recommendation 2

The Act should be restructured, using the Health Privacy Act as a model, so that the information protection principles and exemptions are set out in a Schedule to the Act.

CHAPTER 6

THE INFORMATION PROTECTION PRINCIPLES

INTRODUCTION

6.1 The IPPs regulate the collection, storage, access, use and disclosure of personal information by public sector agencies. A summary of the IPPs follows.

Collection

1. Lawful – only collect personal information for a lawful purpose. Only collect the information if it is directly related to the agency's activities and necessary for that purpose.

2. Direct – only collect information directly from the person concerned, unless they have given consent otherwise. Parents and guardians can give consent for minors.

3. Open – inform the person as to what information is being collected, why it is being collected and who will be storing and using it. Agencies must also inform the person how they can see and correct this information.

4. Relevant – ensure that the information is relevant, accurate, not excessive and up-to-date. Ensure that the collection does not unreasonably intrude into the personal affairs of the individual.

Storage

5. Secure – ensure that personal information is stored securely, not kept any longer than necessary, and disposed of appropriately. Information should be protected from unauthorised access, use or disclosure.

Access

6. Transparent – explain to the individual what personal information about them is being stored, why it is being used and any rights they have to access it.

7. Accessible – allow people to access their personal information without unreasonable delay or expense.

8. Correct - allow people to update, correct or amend their personal information where necessary.

Use

9. Accurate – ensure that the personal information is relevant and accurate before using it.

10. Limited – only use personal information for the purpose for which it was collected; for a directly related purpose; or for a purpose to which the individual has given consent. Personal information may be used without consent in order to deal with a serious and imminent threat to any person’s health or safety.

Disclosure

11. Restricted – only disclose personal information if the person has given their consent or if they were informed at the time of collection that it would be disclosed in this way. Only disclose the information for a related purpose if you believe the person concerned is not likely to object. Only disclose personal information without consent in order to deal with a serious and imminent threat to any person’s health or safety.

12. Safeguarded – do not disclose sensitive personal information without consent, for example, information about a person’s ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership. Only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person’s health or safety.

ANALYSIS OF SUBMISSIONS

6.2 Most respondents accept the underlying principles giving rise to IPPs in the Act. However there is dissatisfaction about the workability of a number of the provisions in the Act.

IPP 1, Lawful Collection (section 8)

6.3 There is little concern amongst public sector respondents with the operation of this IPP, although the Privacy Commissioner suggested that there should be stricter regulation of the *collection* of sensitive personal information.

6.4 While the Annual Reports of Privacy NSW show that collection of personal information is the second most complained about aspect of the IPPs, numbers of complaints about the collection of sensitive personal information are not separately reported.

6.5 Sensitive personal information is not separately defined in the Privacy Act. Section 19 of the Act governs the *disclosure* of certain types of personal information that can be characterised as sensitive, so that disclosure of personal information that relates to a person’s ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities cannot occur unless it is necessary to prevent a serious and imminent threat to the life or health of any person. The collection and disclosure of health information is regulated by the Health Privacy Act.

6.6 National Privacy Principle 10 of the *Commonwealth Privacy Act 1988*, Information Protection Principle 10 of the *Victorian Information Privacy Act 2000* and Information Protection Principle 10 of the *Northern Territory Information Act*

2002 all give special protection to the *collection* of sensitive personal information, so that it cannot be collected unless:

- the individual has consented; or
- the collection is required by law; or
- the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of an individual where the individual is incapable of giving consent or cannot physically communicate consent; or is necessary to establish, exercise or defend a legal or equitable claim.

6.7 Sensitive information is defined in each of these Acts as personal information about a person's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a profession or trade association, membership of a trade union, sexual preferences or practices, or criminal record. Health information is included in the definition in the Commonwealth and Northern Territory Acts.

6.8 The NSW Privacy Commissioner, while noting the existence of protection against the disclosure of sensitive information, supports the adoption of protection against collection of sensitive personal information as the best way of preventing the misuse of such information. However, submissions do not suggest that the lack of protection for collection of sensitive information has caused any practical problems.

Recommendation 3

The Privacy Commissioner should monitor, over a two-year period, whether the lack of protection for collection of sensitive personal information causes significant concerns for citizens, and, if warranted, make further submissions to the Attorney General's Department at the conclusion of the monitoring period.

IPP 2, Direct Collection (section 9)

6.9 Section 9 of the Act provides that an agency must collect personal information directly from the person to whom it relates unless:

- The person has authorised collection from someone else; or
- The information is about a child under the age of 16 and their parent or guardian provides the information.

6.10 The inflexible requirement that the information can only be collected from the person to whom it relates (unless otherwise authorised or compliance would prejudice the interests of the individual to whom the information relates)¹² is unworkable in many situations. Many major human services agencies report that this IPP causes them significant practical problems in the provision of services to their clients.

6.11 The Privacy Commissioner recognises the inflexibility of the current IPP and has made directions under section 41 so that certain public sector agencies may collect personal information from a third party where such collection is 'reasonably relevant and reasonably necessary for the purpose of the agency providing services, diagnosis, treatment or care to the client.'

¹² *Privacy Act*, section 26(1).

6.12 A number of agencies suggest that this IPP should be amended so that personal information is collected from the person concerned if it is ‘reasonable and practicable to do so.’ The equivalent information protection principle contained in the Northern Territory and Victorian Privacy Acts, the Commonwealth’s NPP’s and Health Privacy Principle 3 in the Health Privacy Act are qualified in this way.

6.13 The Privacy Commissioner is supportive of amendment to the principle so that collection from third parties may occur, but only where the information is solely for the purpose of, and reasonably necessary for the provision of services, diagnosis, treatment or care to the client. On the other hand, mirroring the principle in other privacy statutes would contribute to uniformity in the law.

Recommendation 4

Section 9 should be amended so that unauthorised collection from a third party is permitted where it is unreasonable or impracticable to collect the information from the individual to whom the information relates.

IPP 3, Open Collection (section 10)

6.14 Section 10 (IPP 3) requires an agency that collects personal information to notify the individual whose information is collected about:

- the fact of its collection;
- the purposes of the collection;
- the intended recipients of the information;
- whether the provision of the information is mandatory or not, and any consequences of not supplying the information;
- rights of access to and correction of the information; and
- the name and address of the agency that is to hold the information.

6.15 Notification is to be either before, or as soon as practicable after, the collection.

6.16 Generally, submissions to the review did not raise concerns about the application of this principle.

IPP 4, Relevant (section 11)

6.17 Section 11 (IPP 4) of the Act requires an agency to take reasonable steps to ensure that personal information it collects about a person is relevant, accurate and does not intrude on the person’s personal affairs.

6.18 The ADT has determined that “sections 10 and 11 were intended to apply only to the standard case of direct collection. An agency that is not engaged in direct

collection is not subject to the requirements in sections 10 and 11 of the Privacy Act”.¹³

6.19 If the IPP concerning direct collection is amended to permit third party collection then it will also be necessary to ensure that IPPs 3 and 4 apply to the person whose personal information it is, even where the collection is from a third party.

6.20 HPP 4 in the Health Privacy Act specifically provides for the situation where personal information is not collected from the person to whom it relates. In that situation, the agency is bound to ensure that the person to whom the information relates is informed about the collection and about the matters covered in IPP 10 (unless there would be a serious threat to anyone arising from the provision of the advice). NPP 1.3 - 5 of the Commonwealth Privacy Act is in like terms, as are the like Victorian and Northern Territory principles. These are cited as more effective provisions relating to collection notification to the individual whose information it is.

6.21 Even though a like provision in the Privacy Act would not apply to the collection of unsolicited information from the third parties¹⁴ it would add to the administrative obligations of agencies with respect to information that they had asked for. No submissions were received about this issue, probably because the current NSW law does not permit third party collections without consent. If Recommendation 4 is accepted then serious consideration should be given to the fact that the principles in other privacy statutes create an obligation on organisations that collect information about a person from a third party to take reasonable steps to notify the person about the collection, unless serious harm may result.

Recommendation 5

The Act should be amended so that if collection from third parties occurs, the collector should be obliged to take reasonable steps to ensure that the person to whom the information relates is advised of its collection (unless to do so would cause serious harm) and that the information collected is relevant.

IPP 5, Secure storage (section 12)

6.22 Section 12 sets out how personal information is to be retained and secured by agencies. Most respondents did not raise any issues of significance with this provision.

6.23 However, the Ministry for Arts points out that although an exemption from most IPPs is available for records that must be managed in accordance with the State Records Act (in section 25 of the Privacy Act), the exemption does not apply to IPP 5 (section 12).

6.24 The Privacy Commissioner takes the view that section 12(b)¹⁵ is complementary to record keeping obligations on agencies and believes that section

¹³ *HW v Director of Public Prosecutions (No 2)* [2004] NSWADT 73.

¹⁴ Because section 4(5) of the Act provides that ‘personal information is not collected by a public sector agency if the receipt of the information by the agency is unsolicited.’

¹⁵ Which provides that personal information must be disposed of securely and in accordance with any requirements for the retention and disposal of personal information.

12(c)¹⁶ is flexible enough to incorporate industry and government standards on security of information.

6.25 No evidence was provided during the course of the review that there is any conflict in practice between the requirement in the Privacy Act to store and dispose of records securely, and the requirements of the State Records Act. Therefore no recommendation about this issue is made.

6.26 The Privacy Commissioner commented that while section 12 accommodates new storage technologies it fails to provide for secure collection (increasingly important as information is collected electronically) and suggests an amendment to cover this inadequacy. No practical examples of how this problem might arise were provided.

Recommendation 6

The Privacy Commissioner should monitor the security of information collected and stored electronically, and advise the Attorney General of any emerging practical problems with security that cannot be adequately accommodated by IPP 5.

IPP 6, Transparent (section 13)

6.27 Section 13 requires agencies to allow the public to ascertain what personal information is held about them by government.

6.28 Except in the context of the Freedom of Information Act exemptions found in both section 5 and section 20(5) of the Act, this IPP was not the subject of adverse comment by respondents.

6.29 Section 5 states that nothing in the Privacy Act affects the operation of the Freedom of Information Act (FOI Act) and that the Privacy Act does not operate to modify any exemption under the FOI Act or lessen any obligations under that Act in respect of a public sector agency.

6.30 Section 20(5) says that without limiting the generality of section 5 (described above), the provisions of the FOI Act that impose conditions or limitations with respect to any matter referred in sections 13, 14 and 15 (which regulate access to personal information under the Privacy Act) are not affected by the Privacy Act and that the FOI provisions about access apply as if they were Privacy Act provisions.

6.31 These exemptions are discussed in Chapter 10, Specific Exemptions to the Act.

IPP 7, Access (section 14)

6.32 Section 14 requires agencies to provide access by a person to their own personal information in a timely and inexpensive way.

¹⁶ Which provides that personal information must be protected by 'taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse.'

6.33 The way this provision interacts with the Freedom of Information Act 1989 (the FOI Act) may diminish its value in providing easy access to a person's own personal information. The exemptions for the application of the Freedom of Information Act are discussed in Chapter 10, Specific Exemptions to the Act.

IPP 8, Correct (section 15)

6.34 Section 15 creates a right of amendment to a person's own personal information. Similar concerns (discussed in Chapter 10) exist about its value when the application of the FOI Act is considered.

6.35 Section 15(1) compels an agency to ensure that personal information it holds is accurate, relevant, up-to-date and not misleading, and to amend it as necessary, if requested to do so by the person whose personal information it is. Section 15(2) outlines what should happen if an agency chooses not to amend personal information as requested by the person to whom it relates.

6.36 The Privacy Commissioner suggests that these provisions are in conflict and that section 15(2) should be amended to clarify that it applies only if the agency believes the information it holds is accurate and relevant, up-to-date, complete and not misleading and does not warrant amendment. However, agencies generally did not appear to be experiencing difficulties with the provision, suggesting that they are able to accommodate their obligations under both sub-sections without further guidance. No amendment to this Principle is therefore warranted.

IPP 9, Use – information must be accurate (section 16)

6.37 Section 16 obliges an agency to ensure that the personal information it uses is relevant, accurate, up-to-date, complete and not misleading.

6.38 This IPP is not of itself of concern to the majority of respondents. A more detailed discussion of the interrelationship between the use and disclosure provisions follows below.

IPP 10, Use – limited (section 17)

6.39 Section 17 states that an agency holding personal information must not use the information for a purpose other than which it is collected.

6.40 'Use' has been found to mean "to avail oneself of: apply to one's own purposes" by the ADT in *FM v Vice-Chancellor, Macquarie University* [2003] NSWADT 78.

6.41 The section goes on to provide a number of exemptions to the principle where:

- there is express consent (see section 26(2)); or
- it is used for a directly related purpose; or
- it is necessary to prevent serious and imminent threat to the life or health of the individual or another person.

IPP 11, Disclosure – restricted (section 18)

6.42 Section 18 limits the disclosure of personal information. Disclosure is not permitted unless:

- there is express consent (see section 26(2)); or
- it is directly related to the purpose for which the information was collected; and,
- the agency has no reason to believe the person would object to the disclosure; or
- the person is reasonably likely to have been made aware, or has actually been made aware, that information like theirs is usually disclosed to another person or body, or
- the agency 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 person or someone else.

IPP 12, Disclosure – safeguarded (section 19(1))

6.43 Section 19(1) imposes more stringent limits on the disclosure of personal information of an especially sensitive nature. The special restrictions apply to personal information relating to a person’s ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.

6.44 Disclosure of such information will only be permitted with the person’s consent, or if it is necessary to prevent the serious and imminent threat to the life or health of the person or someone else.

USE AND DISCLOSURE PROVISIONS

6.45 The above analysis makes it clear that the provision of different principles for use and disclosure will result in different standards being applied to personal information held by agencies depending on whether they use or disclose it. Generally, the circumstances in which the information can be disclosed will be more limited than the circumstances when it can be used.¹⁷

6.46 The distinction is most stark when issues about use and disclosure arise in large service delivery agencies.¹⁸

¹⁷ This is expressed by the ADT most recently in *NZ v Director General, New South Wales. Department of Housing* [2005] NSWADT 58 at paragraphs 68-71.

¹⁸ For instance, the ADT found, in the case of *KJ v Wentworth Area Health Service* [2004] NSW ADT 84 that “while generally speaking the expression “disclosure” refers to making personal information available to people outside an agency in the case of large public sector agencies consisting of specialised units, the exchange of personal information between units may constitute disclosure.” In that case it was found that the placing of sensitive information, namely psychological counselling notes, on the patient’s general medical file placed the area health service at risk of ‘disclosing’ the information to hospital staff in other units.

6.47 A number of submissions noted that the exemptions to the use and disclosure principles in the Privacy Act are particularly confusing both because they overlap, and because the exceptions to each principle vary

6.48 For instance:

- under section 17 the *use* of information is permitted where it is *directly related* to the purpose for which the information was collected, but
- under section 18 *disclosure* of information is only permitted where it is:
- *directly related* to the purpose for which the information was collected; *and*
- the agency has no reason to believe that the person whose information it is would object to the disclosure (s18(1)(a)).

6.49 Thus, section 18(1)(a) only gives permission to disclose information where it is to be used *for a purpose directly related* to the purpose it was collected for, and not *for the purpose it was collected for* as contemplated in section 17.

6.50 However, disclosure under section 18 is also permitted regardless of whether or not it is directly related to the purpose for which it was collected, if the person was *aware, or was reasonably likely to have been made aware ...* that such information was usually disclosed (s18(1)(b)). Accordingly, it is possible to disclose information in accordance with this provision where *use* of the information in such circumstances would not be permitted.

6.51 If the personal information is sensitive (that is, relating to a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities) then *disclosure* is only permitted where there is a serious and imminent threat to life (section 19(1)). *Disclosure* of sensitive personal information is not permitted in any of the other circumstances permitted in section 18. Yet the use of the same sensitive personal information is not similarly distinguished from the use of other personal information in section 17.

6.52 The practical implications of these variations is succinctly highlighted in the submission from the Department of Health. The Department gives examples of where difficulties with the overlapping and differing exceptions can problems including:

- using/disclosing information to another person or organisation involved in the ongoing care of the patient;
- using/disclosing information to an auditor or quality assessor for the purposes of monitoring, evaluating or auditing the provision of a particular product or service;
- following up complaints about the service or product or recalls of a product;
- following up on an overdue payment, if it related to a service covered by the sensitive information provision; and

- using/disclosing information in the course of managing a legal action or claim brought by the patient.¹⁹

6.53 The separate concepts of use and disclosure in the Privacy Act are rooted in the IPPs in the Commonwealth Privacy Act.

6.54 More recently enacted privacy laws, including the Commonwealth NPPs, and the Victorian and Northern Territory IPPs have consolidated the concepts of use and disclosure so that the principle is expressed to cover use and disclosure together and provides (subject to the coverage of each Act) that personal information must not be used or disclosed for a purpose other than that for which it was collected unless:

- the secondary purpose is related to the primary purpose of collection; and
- the person would have a reasonable expectation that the information would be used for the secondary purpose; or
- the individual had consented to the use or disclosure.

6.55 If the information comes within the category of sensitive personal information then there is a narrower range of circumstances where use or disclosure is permitted.

6.56 Although the Health Privacy Act maintains the distinction between use and disclosure contained in the Privacy Act, it takes the Commonwealth Privacy Act NPPs as its model and applies the same standards to both use and disclosure.

Recommendation 7

The circumstances under which personal information can be used and disclosed should be the same. The use and disclosure principles in the more recent privacy statutes should be used as a model for the reformulation of the Privacy Act principles, although the use and disclosure of sensitive personal information should continue to be treated more restrictively.

CROSS-BORDER FLOWS OF PERSONAL INFORMATION

6.57 Sub-sections 19(2)-(5) deal specifically with the rules relating to disclosure of personal information outside NSW or to a Commonwealth agency.

6.58 Such disclosures are allowed only if they are permitted under a code of practice or the disclosure is made to a jurisdiction that has a 'relevant privacy law'. The Privacy Commissioner is to determine relevant privacy law and publish the determination in the Gazette. To date the Privacy Commissioner has not made a determination under this provision.

6.59 Some individual agency codes of practice permit such disclosures. In other cases cross-border disclosures are permitted pursuant to current section 41 directions.

6.60 Section 19(4) requires the Privacy Commissioner to prepare a Code relating to disclosures outside NSW and to Commonwealth agencies. To date no such code has been made.

¹⁹ NB: Some of these activities are otherwise permitted under a relevant Code, section 41 Direction, or by relying on another exemption in the Act.

6.61 The Privacy Commissioner takes the view that effect of this is that generally speaking the ordinary rules about disclosure apply to trans-border disclosures.

6.62 At least one submission implied that the failure to make a code dealing with cross border flows of personal information exposed NSW to being regarded as a place with less than adequate privacy protections and therefore, less attractive commercially. Since the IPPs in the Privacy Act do not cover the activities of the private sector in NSW, the validity of this implication is questionable.

Recommendation 8

The Privacy Commissioner should:

- Consider the privacy laws that exist in other jurisdictions, with a view to determining their adequacy for the purpose of regulating trans-border disclosures of personal information, and
- Advise the Attorney General (in accordance with a timetable agreed with the Attorney) in relation to the making of a suitable regulation (or code, if the ability to make codes is retained) to regulate trans-border disclosures of personal information.

ADDITIONAL PRINCIPLES

Unique identifiers

6.63 The use of unique identifiers (a code that identifies a particular individual) is set to increase as the technology becomes more accessible for agencies and the demands for ‘whole-of-government’ management of information increase.

6.64 Privacy advocates assert that risks of identity theft and fraud increase with the more common use of unique identifiers, as does the possibility of the sharing of information given for one purpose for a completely different purpose.

Anonymity

6.65 Some people, such as those with mental health disorders, may avoid contact with a service provider because they are concerned about the nature of the personal information that the service provider may retain.

6.66 The Privacy Commissioner suggests that if these people were able to access a government service without revealing their personal details, more serious and costly intervention by service providers at a later date (when the issue for the person may be more difficult to resolve) may be avoided.

6.67 A right to anonymity would also ensure that available technologies are not used by agencies to target otherwise law-abiding citizens, for instance, by using speed cameras to track the daily travel habits of ordinary people.

6.68 The Commonwealth NPPs, Victorian IPPs and Northern Territory IPPs all contain principles relating to unique identifiers and anonymity. Sensibly the

principles are not absolute: they allow for the use of identifiers where it is necessary for the efficient functioning of the organisation; and do not require anonymity to be available where it is not practical.

Recommendation 9

Consideration should be given to incorporating IPPs regulating the use of unique identifiers and preserving the right to anonymity.

CHAPTER 7

CONSENT AND CAPACITY

7.1 The Privacy Act is heavily reliant on the concept of client consent to the management of personal information about them held by agencies.²⁰

7.2 Two issues of concern were raised in submissions.

SUBSTITUTE CONSENT

7.3 Some key service delivery agencies expressed concern about the lack of a substitute consent regime in an Act that is so heavily reliant on client consent.

7.4 In recognition of the difficulties that this can cause for agencies, the Privacy Commissioner has issued best-practice guidelines entitled “*Privacy and People with Decision-making Disabilities.*”

7.5 The guideline was issued by the Commissioner pursuant to section 36(2)(b) of the Act, which gives him the power to prepare and publish guidelines relating to the protection of personal information and other privacy matters. The Act does not give such Guidelines any kind of legislative force.

7.6 One submission to the review suggests that this document, apart from having no legislative force, is too complex to be helpful for people with decision-making disabilities.

7.7 The Health Privacy Act has provisions addressing both assessment of capacity and who can give substitute consent, which are based on provisions in the Victorian Information Privacy Act.

IMPLIED CONSENT

7.8 In the case of *GR v Department of Housing* [2003] NSW ADT 268²¹ the Tribunal concluded that the Department of Housing had no authority to disclose personal information relating to the complainant without obtaining the complainant’s express consent, whether oral or, preferably, written.

20 Section 26(2) of the *Privacy Act* says: ‘A public sector agency is not required to comply with section 10, 18 or 19 if the individual to whom the information relates has expressly consented to the agency not complying with the principle concerned.’

21 GR was a tenant of the Department of Housing. He telephoned a talkback radio program and complained to a researcher about the way the Department had treated him in relation to a particular incident. When the researcher contacted the Department, a Departmental officer told the researcher that GR was a ‘known troublemaker’ and disclosed other, unrelated information about GR. Although the ADT found that GR had given the Department permission to disclose information about the incident to the researcher, it said that this was not permission to talk about the applicant generally or disclose other or unrelated personal information.

7.9 In its submission to the review the Department submits that express statutory recognition of implied consent, which is available at common law, would, in certain circumstances, assist in responding to client concerns.

7.10 The Commonwealth Privacy Act and the Victorian Information Privacy Act define consent to include both express and implied consent.

Recommendation 10

The Privacy Act should provide for both substitute and implied consent to agencies handling a person's personal information in appropriate circumstances.

CHAPTER 8

ENTITIES BOUND BY THE ACT

PUBLIC SECTOR AGENCIES

8.1 The Act defines ‘public sector agency’ at section 3. While the definition is detailed, its scope is not always clear. Ambiguities exist in relation to some individual statutory officers (for example, official community visitors appointed for the purposes of the Community Services (Complaints, Reviews and Monitoring) Act 1993)²² and quasi-government bodies (such as advisory committees and land councils). Other concerns about the definition centre on its application to entities within an agency. That is, are there agencies within agencies, like the relationship between individual schools and the Department of Education and Training. In the case of the Department of Education and Training, this problem is exacerbated by the fact that the definition singles out, from all other government departments, the Education Teaching Service.

8.2 These definitional issues have implications for the application of the regulation of privacy in individual agencies, including:

- an agency’s ability to fulfil its obligations with respect to privacy management plans, annual reporting requirements and the like;
- the liability of an individual statutory officer who is regarded as public sector agency for the purposes of the Act; and
- the application of the IPPs, particularly the use and disclosure principles and exemptions from them.

Recommendation 11

The application of the Act to individual statutory office holders, entities that exist within a larger government agency and quasi-governmental bodies should be clarified by making a regulation that identifies or excludes public sector agencies to which the Act applies.

STATE OWNED CORPORATIONS (SOCS)

8.3 The NSW *State Owned Corporations Act 1989* (the SOC Act) governs State-owned corporations (SOCs).²³

²² Because official community visitors are individuals and do not belong to a larger public sector organization (and therefore lack access to an administrative infrastructure) they are currently the subject of an Order, made by the Attorney General, which exempts them from the obligation to prepare individual privacy management plans. Instead they are covered by the privacy management plan of the Ombudsman’s Office.

²³ The following entities are statutory state owned corporations: Australian Inland Energy Water Infrastructure; Country Energy; Delta Electricity; EnergyAustralia; Eraring Energy; Hunter Water Corporation; Integral Energy Australia; Landcom; Macquarie Generation; New South Wales Lotteries Corporation; Newcastle Port Corporation; Port Kembla Port Corporation; Rail Corporation New South Wales; Rail Infrastructure Corporation; State Water Corporation; Superannuation Administration

8.4 SOCs are specifically excluded from the ambit of the Act. The government's intention in their excluding them was originally to ensure a level playing field so that SOCs did not have to comply with privacy legislation that did not apply to their equivalent service providers in the private sector. Subsequently, the Commonwealth Privacy Act was amended to include the large companies in the private sector, however the application of the Commonwealth Act to state instrumentalities is incomplete, as they must either be incorporated under the Corporations Act 2001 (Cth) or prescribed as organizations for the purpose of the Commonwealth Privacy Act before it will apply. To date only four NSW SOCs have been prescribed, namely:

- Australian Inland Energy Water Infrastructure,
- Country Energy;
- Energy Australia; and
- Integral Energy Australia.

8.5 Very few SOCs made substantive submissions to the review. The most common concerns were that they not be subject to more than one privacy regime, and the need for competitive neutrality with private sector competitors. However, many larger private corporations are now obliged to conform with the Commonwealth Privacy Act NPPs. Further, SOCs have a number of statutory objectives, not just to be a successful business and operate at least as efficiently as a comparable business (section 20E(1)(a)), but also 'to exhibit a sense of social responsibility by having regard to the interests of the community in which [they] operate' (section 20E(1)(b)).

8.6 SOCs that are covered by the Commonwealth regime were concerned that duplication of privacy regulation should not occur. At least one SOC submission specifically stated that the exclusion of SOCs from the Privacy Act should be maintained.

8.7 Although no submissions were received from unregulated SOCs indicating that they wished to be covered by the state law, the Privacy Commissioner notes that not all SOCs are comfortable with this state of affairs. In particular, the Commissioner reported that Sydney Water would prefer to be regulated with respect to its privacy obligations and has decided to voluntarily comply with the IPPs as a matter of customer respect and trust.

8.8 Conversely, some SOCs want to be included in the coverage of the Privacy Act so that they are able to take advantage of current exemptions relating to the transfer of personal information between agencies, and so that other agencies could disclose personal information to them.

8.9 The Privacy Commissioner submits that being included in the coverage of the Privacy Act is desirable for reasons of public credibility and to enable information sharing to occur under the auspices of the law enforcement and investigations exemptions to the IPPs in the Act.

Recommendation 12

All NSW SOCs should be subject to privacy regulation, so that either:

- The NSW Privacy Act should apply to SOCs that are not covered by the Commonwealth Privacy Act, or
- Their prescription under the Commonwealth Act should be facilitated.

GOVERNMENT CONTRACTORS

8.10 The application of the Privacy Act to non-government organizations (NGOs) that contract to provide government services (beyond section 3(g), which includes a person or body providing data services to a public sector agency in the definition of ‘public sector agency’) is not provided for in the Act.

8.11 Some agencies deal with the question of an NGO’s liability for breaches of the Privacy Act in the terms of any contract between them, and the Commonwealth Privacy Act regulates some private contractors. However, there is a view among some stakeholders that these forms of coverage are an inadequate means of providing individual privacy protection, especially when the individual is initially the client of the government service delivery agency. In an environment where government services may increasingly be delivered by an outside contractor a reconsideration of this issue in the privacy context is warranted.

8.12 Section 17 of the more recent Victorian Information Privacy Act 2000 and section 95 of the Commonwealth Privacy Act specifically provide for the effect of outsourcing on the obligations of agencies under those Acts.

8.13 In Victoria a contract between the outsourcing State organization and a contracted service provider can require the service provider to adhere to the IPPs and any applicable code of practice when providing the contracted service in the same way and to the same extent that the outsourcing State organization would have been bound if it provided the service directly. The outsourcing organization and the contracted service provider are jointly liable for the acts of the service provider unless a contract exists and it is possible to enforce the IPP or code of practice against the contracted service provider. The usual agency provisions in the Act do not apply where there is a contract.

8.14 The Commonwealth Privacy Act provides (at section 95B) that a contracted service provider stands in the shoes of the agency that has contracted with it for the purpose of adherence to the IPPs, and requires that the contract be drafted so as to exclude the possibility that the service provider may be required to breach the IPPs. Sub-contractors are also specifically regulated. This formulation of the contracted service provider’s obligations appears simpler than the Victorian formulation, although both provisions merit consideration.

Recommendation 13

The Act should provide a structure for binding non-government organisations that are contracted by public sector agencies to provide services that require the management of personal information to conform to the terms of the Privacy Act, unless a privacy law equivalent to the terms of the NSW Privacy Act otherwise binds them. A regulation nominating equivalent privacy laws should be made.

CHAPTER 9

PERSONAL INFORMATION

PERSONAL INFORMATION DEFINED

9.1 The Privacy Act applies to personal information. Personal information is defined as “information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.” It includes “such things as an individual’s fingerprints, retina prints, body samples or genetic characteristics.”

9.2 Most respondents did not comment directly on the adequacy of the definition, although a number had concerns about the nature of exemptions to the definition. Nevertheless there is some concern that agencies and the public struggle with the concepts in the definition and clarifying amendments have been proposed:

- to make it clear that personal information need not be recorded in a data base; and
- to more clearly assert that photographic images and video footage can constitute personal information.

9.3 The Privacy Act definition of personal information is an expansive one. It is comparable to that found in the Commonwealth Privacy Act and the Victorian Information Protection Act.

9.4 Submissions from agencies to the review often expressed uncertainty about how they were to comply with a number of the IPPs, especially those set out in sections 12, 13, 14, 15 and 16, if information is only held in the minds of individual officers.

9.5 The Court of Appeal²⁴ has recently determined that “The primary context of the legislation which gives meaning to the words ‘holds personal information’ strongly indicates that the words do not extend to the information held within the mind of an employee.”²⁵ It has found that personal information is ‘held’ when it is in the possession or control of an agency, an employee or other person acting in the course of such employment or engagement with the agency and that it does not extend to material held only in the mind of a person.²⁶ The Court has taken the view that the reference to ‘material form’ in the definition of personal information “should be taken as intended to ensure that electronic databases are covered by the legislative scheme.”²⁷

24 *Vice-Chancellor Macquarie University v FM*, NSW Court of Appeal, 10 June 2005, File No 40926/03, unreported.

25 *ibid* at Held per curium, para 8.

26 *ibid* at Judgement, para 34.

27 *ibid* at Judgement, para 27.

9.6 The findings of the Court of Appeal address the concerns expressed by many respondents about the consequences of the earlier ADT Appeal Panel decision in the Macquarie University case.²⁸

9.7 As the Court has found, “It is impossible to conceive how most of ss 12-19 could apply to information in the minds of employees.” And, further: “It seems likely that the scope of personal information is the same for the obligations relating to ‘collection’ as it is for those relating to ‘holding’ and ‘disclosure’.”²⁹

Recommendation 14

Using the decision of the Court of Appeal in *Vice-Chancellor Macquarie University v FM* as a guide, the Act should be amended so that it is clear that the IPPs do not apply to personal information held in the minds of employees.

EXEMPTIONS TO THE DEFINITION OF PERSONAL INFORMATION

9.8 Exemptions to the definition of personal information take a particular class of personal information outside the scope of the Act altogether.

Section 4(3) says that personal information does not include:

- a) information about an individual who has been dead for more than 30 years;
- b) information about an individual that is contained in a publicly available publication;
- c) information about a witness who is included in a witness protection program under the *Witness Protection Act 1995* or who is subject to other witness protection arrangements made under an Act;
- d) information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth;
- e) information about an individual that is contained in a protected disclosure within the meaning of the *Protected Disclosures Act 1994*, or that has been collected in the course of an investigation arising out of a protected disclosure;
- f) information about an individual arising out of, or in connection with, an authorised operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*;
- g) information about an individual arising out of a Royal Commission or Special Commission of Inquiry;
- h) information about an individual arising out of a complaint made under Part 8A of the *Police Service Act 1990*;
- i) information about an individual that is contained in a document of a kind referred to in clause 1 or 2 of Schedule 1 (restricted documents) to the *Freedom of Information Act 1989* (i.e. Cabinet documents or Executive Council documents);
- j) information or an opinion about an individual’s suitability for appointment or employment as a public sector official;

²⁸ *Vice Chancellor, Macquarie University V FM* [2003]NSWADTAP 43.

²⁹ NSW Court of Appeal, *op cit*, Held, paras 2 and 4.

ja) information about an individual that is obtained about an individual under Chapter 8 (Adoption information) of the *Adoption Act 2000*;

k) information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations for the purposes of this subsection.

Section 4A of the Privacy Act exempts health information as defined in the Health Privacy Act.

9.9 Generally, respondents had little or nothing to say about the section 4(3) exemptions although the Privacy Commissioner commented that it would be preferable for the exemptions to be more limited, by reference to IPPs which should not apply, rather than taking those types of personal information outside of the scope of the Act altogether. The Commissioner also noted that many of the exemptions (particularly those relating to information about protected witnesses, information collected through telephone interceptions and information concerning adoptions) relate to matters that would otherwise be subject to tough sanctions for corrupt disclosure.

9.10 The exemptions for personal information:

- about an individual who has been dead for more than 30 years;
- about an individual that is contained in a publicly available publication; and
- about an individual's suitability for appointment or employment as a public sector official.

were, however the subject of submissions by some respondents.

An individual who has been dead for more than 30 years.

9.11 This exemption means that the Act applies only to personal information about an individual who is alive, or who has been dead for less than 30 years.

9.12 The length of time for which an individual's personal information is covered by the Privacy Act has practical implications for some service providers, particularly since the Act is so heavily dependent on a person's consent to use or disclose their information, and there is no provision for substitute consent.

9.13 One submission suggested that the timeframe should be reviewed and reduced, although the respondent noted that problems with the lengthy time period were rare in practice and to date had been managed by reference to other access to information regimes.

9.14 Another submission suggested that the personal information concerning deceased persons should only be protected if it can also refer to a living person, such as in the case of genetic conditions.

9.15 In the context of these submissions it is noteworthy that Health Privacy Act adopts the same exemption for people who have been dead for more than 30 years, even though it is in the area of health information that the practical ramifications of

such a long period of privacy protection (for those who have been dead less than 30 years) are most likely to cause difficulties.

9.16 While there maybe difficulties with the provision, at this stage, the issues raised do not warrant a change to the Act. It may be more appropriate to explore these difficulties in the context of the application of the State Records Act. In any event, the effect of the provision, and its interaction with the State Records Act, should be monitored.

Publicly available publication

9.17 The Privacy Commissioner is concerned about the broad nature of this exemption and suggests that it has the potential to undermine the objects of the Act. This concern could be addressed by removing the general exemption in favour of a specific exemption from IPP 2 (which governs where information can be collected from).

9.18 There is particular concern that the exemption can be interpreted as a ‘public domain’ type exception and that the internet increases the risk of inaccurate information, or accurate information being taken out of context. Perhaps in an attempt to address this issue the ADT Appeal Panel has said that “meaning is gleaned from both the content and the context in which information or an opinion appears” and therefore “a name and address in a telephone directory conveys different information to the same name and address held in the file of a child protection agency.”³⁰

9.19 A small number of respondents were of the view that the exemption does give an incentive for agencies to act contrary to the spirit of the Act in some circumstances. For example some respondents noted that it would be possible for an agency to release information to the press, and then claim that, because it had been published, it was exempt from the Act. Of course, such a strategy would almost certainly put the agency in breach of the IPPs concerning disclosure, and possibly use as well.

9.20 If agencies continue to apply the exemption sensibly and in the spirit of the Act, so as to apply the IPPs and protect the privacy of individuals, then no action is required. If agencies begin to make unreasonable claims about the nature of the information they manage, then the exemption should be reviewed.

Suitability for appointment or employment as a public sector official

9.21 The ADT interpreted this provision to mean that “The information in issue must be able to be shown to be information ‘about suitability.’ It must contain within it language which indicates to an objective observer that the information canvasses the aptitude and competence of the employee with respect to their current or prospective employment ... If this approach is adopted, then it would be an unusual case where

³⁰ See *Commissioner of Police, New South Wales Police v EG; EG v Commissioner of Police, New South Wales Police* (GD) [2004] NSWADTAP10.

the exclusion would apply outside what I have described as the routine personnel context (that of recruitment, promotion, discipline and involuntary retirement).”³¹

9.22 The Privacy Commissioner has submitted that the exemption goes well beyond the intention of the parliament to allow for free and frank discussion during the public sector employee selection process. The 2002-2003 Annual Report of the Commissioner reports that 18% of all complainants against NSW public sector agencies and 15% of all internal review applicants were employees of the agency. However, there is no substantive case law to indicate that the exemption is working in a way different from that which parliament intended.

9.23 The ADT’s interpretation of the exemption may bring it more into line with the Commonwealth Privacy Act exemption for employee records held in the private sector. Employee records privacy is currently the subject of joint investigation by the Commonwealth Attorney General’s Department and the Department of Employment and Workplace Relations. Consideration of the Privacy Commissioner’s position could be revisited once the work of that investigation is complete.

9.24 Law enforcement exemptions

9.25 Generally, respondents did not express concern about most of the specific law enforcement exemptions in section 4(3). However, the Privacy Commissioner submitted that they should be reconsidered in light of the operation of other law enforcement exemptions contained in the Act in consultation with relevant agencies, with a view to rationalising them.

9.26 NSW Police made a submission to the review (supported by the Ombudsman) about the ADT’s recent interpretation of the exemption at section 4(3)(h) which exempts information about an individual arising out of a complaint made under Part 8A of the *Police Service Act 1990*. Part 8A deals with complaints about the conduct of police officers.

9.27 The ADT³² has interpreted the exception in section 4(3)(h) narrowly, but in accordance with its ordinary meaning and found that it “will only apply to information which results or proceeds from a complaint and is relevant to that complaint.”

9.28 In another case³³ a differently constituted Appeal Panel, interpreting the words ‘arising out of’ in section 4(3)(h) said “As we see it, what is required to be shown is that the information in issue has ‘resulted’, proceeded or originated from a complaint made under Part 8A” and “... the exclusion would not protect information that had an indeterminate or tenuous relationship – and, a fortiori, not a relationship at all – with the investigation.”

9.29 Even though the Police acknowledge that such an interpretation may exclude more personal information dealt with in the context of Part 8A complaints from the

³¹ See: *Y v Director General, Department of Education & Training* [2001] NSWADT 149.

³² in *GA & Ors v Department of Education and Training and NSW Police* (GD) [2004] NSW ADTAP18.

³³ *KO & anor v Commissioner of Police, New South Wales Police* (GD) [2004] NSWADTAP21.

ambit of the Act than the requirement that it be relevant in order to be excluded, they remain concerned that the condition that the information ‘arising out of’ a complaint be *relevant* is a narrower interpretation of the provision than was intended by the legislature. They submit that it will have an adverse effect on the prevention and investigation of matters of police corruption because “at any one time it is difficult to determine whether a particular piece of information is going to be relevant or not.”

9.30 When taking into account the overall objective of the Privacy Act to protect the privacy of individuals, the ADT’s determination that the personal information be relevant to the Part 8A investigation if it is to be excluded from the ambit of the Act does not seem overly onerous. Furthermore, the Police are entitled to rely on the specific law enforcement and investigative exemptions set out in Part 2 Division 3 of the Act, as well as section 27, which specifically exempts certain named law enforcement agencies from the application of the IPPs, other than in connection with their administrative and educative functions. The section 23, law enforcement exemptions, section 24, exemptions for investigative agencies and section 27 exemptions are discussed in Chapter 10.

9.31 At this time there does not seem to be sufficient justification for amendment of the provision as suggested.

Should personal information held by cultural institutions be excluded from the ambit of the Act?

9.32 The Ministry for the Arts has expressed the view that the state’s cultural institutions should be exempt from the IPPs so that they can operate on the same basis as their counterparts in other jurisdictions. It has been recommended that the Act be amended so that it mirrors the Health Privacy Act by excluding from the definition of personal information:

- information about an individual that is contained in a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition,
- information about an individual that is contained in a State record under the control of the State Records Authority that is available for public inspection in accordance with the State Records Act 1998;
- information about an individual that is contained in archives within the meaning of the Copyright Act 1968 of the Commonwealth;

9.33 Currently, cultural institutions are able to operate without adherence to most IPPs, by virtue of a section 41 direction which exempts the application of certain IPPs to personal information that is held by a public sector agency for research purposes.

9.34 The section 41 direction applies to:

- the disclosure of personal information held by an agency for research;
- the collection storage, use, disclosure, provision of access to, and alteration of personal information that was created or collected by people or organizations that were not public sector agencies but was subsequently deposited with the public sector agency for purposes including research; and

- the collection and use of personal information by agencies that are primarily concerned with the collection of items of historical and cultural significance where the information is collected to provide reference material in relation to the collected items.

9.35 The direction then goes on to put further qualifications on the application of the exemptions from particular IPPs.³⁴

9.36 The direction has a broad coverage, so that any (named) public sector agency is protected from the application of the IPPs when engaged in research. Use of deposited material is conditional on reasonable steps being taken to protect the privacy of individuals and the collection and use of historical or culturally significant items requires a written policy on privacy protections to be in place.

9.37 The Ministry for Arts submission is that the Act should be amended and that a regulation should be made to ensure exemption from compliance with the IPPs for cultural institutions in the interim. It has the support of the NSW Branch of the Australian Society of Archivists

9.38 In response to this proposal, a regulation has been drafted which adopts a broad exception to the definition of personal information and applies it to agencies that are State collecting institutions for the purpose of the State Records Act³⁵ and all local libraries. The draft regulation excludes all provisions of the Privacy Act, instead of following the model in the section 41 direction which exempts the application of certain IPPs on certain conditions. It has not been progressed pending this review.

9.39 If the proposed amendment (either by way of amendment to the Act or by the making of regulation) is implemented, it will have the effect of exempting personal information (rather than just the application of relevant IPPs, with conditions) held for the purposes of reference, study or exhibition, or pursuant to the State Records Act, or contained in an archive as defined in the Copyright Act from the ambit of the Act. This is a broader exemption than that achieved by the existing section 41 Direction, while covering a smaller group of agencies.

9.40 The Commonwealth Privacy Act has a similar exemption (from the definition of record), as does the Victorian Information Protection Act. The Health Privacy Act adopted the same exemption and builds exemptions for research and investigations into its HPPs. Statutory guidelines support the exemptions.

Recommendation 15

The provisions of the section 41 Direction about research (suitably updated) should be incorporated into the Act. Otherwise, a regulation with this effect should be made.

³⁴ The full text of the section 41 direction may be accessed on the Privacy Commissioner's website.

³⁵ That is: the Art Gallery of NSW Trust, the Australian Museum Trust, the Historic Houses Trust of New South Wales, Trustees of the Museum of Applied Arts and Sciences, National Parks and Wildlife Service, Royal Botanic Gardens and Domain Trust, Library Council of New South Wales (in respect of the State Library of New South Wales), the Sydney Opera House Trust, the Zoological Parks Board and any other prescribed institution.

COLLECTION OF UNSOLICITED INFORMATION

9.41 Section 4(5) of the Act provides that personal information is not collected if it is unsolicited.

9.42 In the recent ADT decision of *KD v Registrar, NSW Medical Board* [2004] NSWADT 5, the Tribunal determined that section 4(5) means that the use and disclosure IPPs (in sections 17 and 18) do not apply to personal information that was not collected. The President of the ADT thought it unlikely that section 4(5) was meant to place personal information that, although unsolicited, is subsequently stored, used and disclosed by an agency beyond the ambit of the IPPs. This view is reflected in the more recent ADT case of *HW v Director of Public Prosecutions (No 2)* [2004] NSWADT 73.

Recommendation 16

The Act should be amended to clarify that while unsolicited information is not subject to the collection principles, the other IPPs do apply.

OTHER CATEGORIES OF SENSITIVE PERSONAL INFORMATION

9.43 The Privacy Commissioner raises the possibility of expanding and refining the categories of sensitive personal information governed by the Act. In particular, he submits that criminal records should be included in the definition of sensitive personal information and that the meaning of ‘sexual activities’ be clarified. No other submissions were received concerning these matters, although it is noted that the Privacy Commissioner’s annual reports reflect that treatment of a person’s criminal record is a common complaint to Privacy NSW.

9.44 The legislation in NSW governing criminal records deals only with spent convictions. It is appropriate for privacy legislation to protect personal information concerning a person’s criminal record, if it is not otherwise protected. The privacy laws in Victoria, the Northern Territory and the Commonwealth all include criminal records in the definition of sensitive personal information.

9.45 There is no evidence to suggest that meaning of ‘sexual activities’ has led to difficulties in the privacy protection of sensitive personal information to date. However, the fact that complaints concerning criminal records make up a sizeable number of complaints to the Privacy Commissioner suggests that privacy protection for this class of sensitive personal information is warranted.

Recommendation 17

The definition of sensitive personal information in the Act should include a person’s criminal record.

CHAPTER 10

SPECIFIC EXEMPTIONS TO THE ACT

JUDICIAL FUNCTIONS AND ACCESS TO COURT RECORDS

10.1 A number of respondents made submissions about privacy protection of court records. There was particular concern expressed about the lack of protection available for judgments published on the Internet. The Privacy Act provides a number of exemptions that accommodate the management of personal information by courts. In particular, section 6 excludes the judicial functions of courts and tribunals and the functions of a Royal Commission or Special Commission of Inquiry from the ambit of the Act.

10.2 Section 14B of the Electronic Transactions Act, which establishes an electronic case management (ECM) system for the courts, provides that for the purposes of the *Freedom of Information Act 1989*, the *Privacy and Personal Information Protection Act 1998* and the *State Records Act 1998*, information contained in the ECM system with respect to proceedings in an ECM court (including proceedings that have been finally disposed of) is taken to be information concerning the judicial functions of that court.

10.3 Reference to the specific law enforcement, investigations and ‘other laws’ exemptions from the IPPs contained in the Act may also assist in determining the application of the Act to court records in circumstances where section 6 does not apply.

10.4 The Privacy Commissioner takes the view that the administration and publication of court lists, registry decisions in relation to application forms and processes, determinations about access to and publication of court files should be defined as non-judicial functions. However, subjecting this information to regulation by the Privacy Act may mean compromising the public interest in the maintenance of an open, transparent justice system.

10.5 The recent NSW Law Reform Commission Report on Contempt by Publication makes recommendations about access to court records. The Chief Justice has asked the Attorney General to consider legislating this area and developing a cross-jurisdictional approach.

10.6 The NSW Attorney General’s Department is conducting a separate review of this issue.

RECORDS MANAGED UNDER THE *STATE RECORDS ACT 1998*

10.7 When the Act was debated in parliament, a number of speakers expressed concerns about the application of the Act to personal information held in State records. Historians and genealogists were concerned that the Act had the potential to restrict their access to historical and family history records. Consequently the

government amended the Act to clarify the relationship between the State Records Act and the Privacy Bill. The amendments had the support of the State Archives Authority and the History Council.

10.8 Section 25 of the Act exempts public sector agencies from the IPPs set out in sections 9,10,13,14,15,17,18 or 19 if “non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).”

10.9 The effect of this exemption is to apply the State Records Act to records that come within its regulation to the exclusion of the IPPs (except section 12) of the Privacy Act. There is no practical problem arising from the fact that section 12 is excluded from the exemption. Submissions concerning the issue are discussed in Chapter 6, under the heading *IPP 5, Secure storage*.

10.10 Notwithstanding this general rule that the State Records Act will apply to records covered by that Act, section 15(4) of the Privacy Act does apply section 15 (which provides a regime for the alteration of personal information held by an agency) and any code of Practice concerning the alteration of personal information to records ‘despite section 25 of this Act and section 21 of the State Records Act 1998.’

10.11 Section 15(4) was introduced into the Privacy Act by way of an amendment to the Act in the Health Privacy Act in 2002 so as to clarify that the rights to amendment of a person’s own personal information set out in section 15 override the obligations to protect state records set out in section 21 of the State Records Act.

10.12 Section 15 requires agencies to “make appropriate amendments (whether by way of correction, deletions or additions) to ensure that the personal information is accurate, relevant, up to date, complete and not misleading.” Some respondents felt these rights did not go far enough and took the view that there should be a right of complete expunction. However, section 15(1) does contemplate amendment by deletion to ensure accuracy. Presumably that may amount to expunction of the record in certain circumstances.

10.13 The Ministry of Arts has acknowledged that “While the provisions relating to personal information in the (Privacy) Act and the State Records Act are very different, *they do not generally conflict in practice*” (emphasis added). Nevertheless, there is a perception amongst agencies that the Privacy Act and the State Records Act somehow conflict, or that the all IPPs in the Privacy Act should be applied to records managed under the State Records Act, even though:

- Section 25 specifically provides that the State Records Act applies in preference to the Privacy Act, with the exception that section 15(4) of the Privacy Act which governs how personal information held in a state record can be altered; and
- Personal information as defined in the Privacy Act is only one kind of state record governed by the State Records Act.

10.14 The fact that there is no conflict in practice means that it can be concluded that the terms of the Act remain appropriate. Therefore, no amendment to the relevant provisions is required.

10.15 A co-operative working relationship between the Privacy Commissioner and the State Records Authority should assist in developing a public sector that is well-informed about its record-keeping obligations.

FREEDOM OF INFORMATION ACT EXEMPTIONS

10.16 Section 5 of the Privacy Act says that nothing in it affects the operation of the Freedom of Information Act, and particularly that the Privacy Act does not:

- modify any exemption under the FOI Act; or
- lessen any obligations under that Act in respect of a public sector agency.

10.17 Section 20(5) of the Privacy Act provides that “Without limiting the generality of section 5, the provisions of the Freedom of Information Act 1989 that impose conditions or limitations (however expressed) with respect to any matter referred to in section 13, 14 or 15 are not affected by this Act, and those provisions continue to apply in relation to any such matter as if those provisions were part of this Act.”

10.18 The application of these provisions is of concern to many public sector agencies and other stakeholders, most notably the Ombudsman, the Privacy Commissioner, the Department of Local Government, local councils and the larger service delivery agencies.

10.19 The way in which the provisions are put into practice by agencies varies across the public sector. Some agencies treat all applications for access to personal information as applications under the Freedom of Information Act 1989 (FOI Act). This has consequences for the applicant including:

- variation in time limits for applications to be made, dealt with and reviewed;
- variation in the ability to charge for work associated with accessing and amending records; and
- accessibility of jurisdiction for external review.

10.20 Others entertain applications under the Privacy Act, where the process might be regarded as more flexible for applicants but more difficult for agencies to manage.

10.21 The discrepancies concerning time, cost, flexibility and jurisdiction are even more marked where an application under the Local Government Act 1993 (LG Act) is available. Section 12 of that Act requires the provision, free of charge, of a number of documents held by councils that may contain personal information that would (except for the ‘other laws’ exception in section 25 of the Privacy Act) be protected by the application of the IPPs. Further, section 12(6) of the LG Act allows council officers to decide to release documents not otherwise mandated for release under section 12 if the officer is satisfied that it is in the public interest to do so. In determining the public interest, council officers are advised by the Department of Local Government to consider privacy principles. The facts in the ADT case, *NV v Randwick City Council* [2005] NSWADT 45, illustrate some of the tensions in the regulation of access to information inherent in the competing statutory requirements of the Privacy Act and the LG Act.

10.22 Some respondents suggest that all access and amendment issues should be dealt with in the Privacy Act, while others recommend that access and amendment provisions in the Privacy Act should be repealed and these issues be dealt with under the FOI Act. All the submissions point to a clear preference for access and amendment information held by the public sector, including personal information, to be governed by a single Act.

10.23 There is little uniformity in the way other States or the Commonwealth manage the relationship between privacy and access to information laws. When this issue was considered in the context of enacting the Health Privacy Act, the parliament determined to maintain the same relationship between FOI and privacy as is provided for in the Privacy Act in relation to the public sector.

10.24 The Ombudsman's concerns about the inter-relationship between the access to information regimes in FOI, privacy and local government have also been discussed in other public forums, most notably in his recent Annual Reports and before the Inquiry into Access to Information conducted by the former Parliamentary Committee on the Office of the Ombudsman and the Police Integrity Commission (the Committee).

10.25 The first report on the Inquiry, published by that Committee in December 2002, accurately identifies that "while some core areas of agreement exist (between the Ombudsman, local government stakeholder representatives and the Department of Local Government) different views are found as to the scope and precise nature of the problems concerned."³⁶ This is also true of submissions to this review.

10.26 The Parliamentary Committee reviewed the question of overlap and potential conflict between the access to information regimes and identified problems with the interaction between the three schemes.³⁷ It deferred decisions about the continuation of its Inquiry pending the outcome of a number of reviews and inquiries.

10.27 Nevertheless, the Committee stated that it believes that "more independent evaluation is needed of the way in which the three schemes interact in order to enable informed decision making on the best way to reform and rationalise the three schemes in place."³⁸ It noted past unfavourable assessments of the operation of the FOI legislation by the Ombudsman who has previously called for a comprehensive review of the legislation to ensure its continuing relevance in the electronic age.

10.28 Options for reform suggested by respondents to this review include:

- Explicitly provide that access and amendment applications will be dealt with under the FOI Act so that one set of provisions applies to all access and amendment issues. The Victorian Information Privacy Act takes this route.

³⁶ NSW Parliament, Committee on the Office of the Ombudsman and the Police Integrity Commission, First Report on the Inquiry into Access to Information, p 21.

³⁷ see *ibid*, p 38.

³⁸ *ibid* page 40.

- Establish a more comprehensive process for access and amendment of all personal information in the Privacy Act. A precedent for this strategy can be found in the private sector provisions of Health Privacy Act.

10.29 It is clear that agencies are looking for a single regime to govern the release of information held by them.

Recommendation 18

A single set of rules (which take into account the existing regimes in the FOI, Privacy and LG Acts) for managing access to, and alteration of information, including personal information, held by the public sector should be developed and legislated.

Section 23: law enforcement exemptions and section 24: exemptions for investigative agencies

10.30 Section 23 provides exemptions for the activities of both defined law enforcement agencies and agencies that collect, use or disclose personal information for some law enforcement and associated functions. Section 24 provides exemptions for both defined investigative agencies and agencies dealing with complaints and other matters that can be referred to an investigative agency.

10.31 The law enforcement exemption covers five different IPPs, both law enforcement agencies and all agencies, and uses nine different tests. The Privacy Commissioner is concerned that terms ‘law enforcement’ and ‘for the protection of public revenue’ may be interpreted so that the exemption applies to law enforcement processes beyond breaches of the criminal law and preparation of cases before courts and tribunals. On the other hand some agencies that are engaged in law enforcement that is not of a criminal nature are concerned that the exemption does not apply to them.

10.32 In a recent case which concerned a possible breach of the disclosure IPP in the course of an investigation into a medical practitioner for alleged misconduct, the ADT has determined³⁹ that: *“In my opinion, the term “law enforcement” should be given its ordinary meaning and should not be narrowly construed. ... I am also of the view that disciplinary action, pursuant to an Act of Parliament, for breaches of professional standards comes within the term ‘law enforcement’.”*

10.33 Similarly, the investigations exemption covers five different IPPs, investigative agencies (as defined), two additional named agencies and all agencies, and uses five different tests. Part of the exemption has now been made redundant by complaint, referral and information sharing provisions of the Ombudsman Act.

10.34 Generally, respondents are concerned about the general and generic nature of the exemptions. Many respondents suggest that their particular functions are not covered by the exemptions and that the exemptions apply unevenly depending on the actual conduct of the agency in each case. For example, one respondent notes that although section 24 (3) allows disclosure of information, without adherence to the relevant IPP, between investigative agencies, it is not clear that the same disclosure by

³⁹ in the case of *JD v Director General, NSW Department of Health* (No.2) [2004] NSW ADT 227.

a law enforcement agency to an investigative agency would be similarly exempt by virtue of section 23(5). Consequently, even if the Privacy Act identifies certain agencies as law enforcement and/or investigative agencies, the application of relevant law enforcement or investigations exemptions to their activities will need to be considered in each case.

10.35 The limitations of the exemption for investigations conducted by and within public sector agencies that are not primarily investigative agencies, including inability to brief counsel or consult experts in the course of an investigation, have been recognised. To assist in resolving these difficulties in the short term, a section 41 direction relating to all agencies' investigative functions is in place.⁴⁰ A separate section 41 direction permits the release of information by agencies for certain purposes relating to dealing with correspondence and inquiries as well as performance audits.

10.36 The Ombudsman has made a specific submission concerning the inability of that office to obtain personal information from agencies unless a formal investigation is mounted. This hinders the ability of that Office to resolve certain complaints on an informal basis (pursuant to section 13AA of the Ombudsman Act which gives powers to conduct preliminary inquiries). This submission highlights the fact that the exemptions for investigative agencies only extend to other agencies if they are investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency or that has been referred from or made by an investigative agency.

10.37 The exemptions for both law enforcement and investigative functions are more clearly focused in the Health Privacy Act. In particular, the Health Privacy Act exemption for law enforcement agencies is restricted to circumstances where there are reasonable grounds to believe that an offence may have been, or may be committed. The exemption for investigative agencies permits disclosure of information where it is reasonably necessary for the exercise of complaint handling or investigative functions of an investigative agency and for general agencies conducting investigations in relation to their staff and the like.

⁴⁰ The coverage of this section 41 Direction was recently interpreted by the ADT. The Tribunal found that the Direction only covers the conduct of the investigating agency, not the responding agency, see *NW v New South Wales Fire Brigades* [2005] NSW ADT 73.

Recommendation 19

- The exemptions for law enforcement and investigative functions in sections 23 and 24 should be simplified and applied in a similar manner to the like exemptions in the Health Privacy Act.
- Investigations concerning disciplinary proceedings and professional misconduct and the like should be specifically included in the exemptions.
- The section 41 directions relating to investigations and information sharing should likewise be incorporated into the exemptions in the Act. The exemptions should allow for a flow of information to and from an investigating agency and specifically permit the sharing of information by agencies for the purpose of briefing counsel and consulting other experts.

Section 25 – exemption where non-compliance lawfully authorised

10.38 Section 25 of the Privacy Act permits non-compliance with some IPPs if an agency is:

- lawfully authorised or required not to comply with the principle concerned, or
- the non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

10.39 The scope of this exemption is broad and, in the view of some respondents, is relied on by agencies so that the objectives of the Privacy Act are effectively undermined. In particular the Privacy Commissioner submitted that “section 25 has the effect of subordinating a privacy law intended to confer general rights and have general application, to laws limited to specific situations in a way which undermines public expectations and produces wide ranging uncertainty.” The Commissioner suggests that the exemption should be narrowed to a provision, which gives priority to other legislation only in cases of express inconsistency, and that agencies should be required to establish ‘reasonable necessity’ in order to justify non-compliance.

10.40 Although this exemption might be used by agencies as a ‘catch-all’ provision, it allows privacy concerns to be addressed in an agency specific way in other legislation. As there is nothing to suggest that this provision is working other than as Parliament intended, there is no need for amendment to its terms.

Section 27 – specific exemption for ICAC, Police Service, PIC and NSW Crime Commission

10.41 This exemption means that ICAC, the Police Service, the Police Integrity Commission and the NSW Crime Commission only have to comply with the information protection principles in pursuit of their administrative and educative functions.

10.42 The Privacy Commissioner suggests that, in relation to this exemption, the purpose set out in the second reading speech “ ... not to protect secrecy in dealings or to protect the Government from accountability” could be better achieved by defining

more closely the exemption for watchdog bodies, so that their legitimate law-enforcement activities are protected from undue scrutiny pursuant to privacy legislation, but are otherwise subject to the IPPs.

10.43 Conversely, NSW Police seek an amendment to ensure that their investigative functions (such as those under Part 8A of the Police Service Act) are not subject to the Privacy Act.

10.44 The Appeal Panel of the ADT⁴¹ has expressed a provisional view about the application of section 27 in the context of Part 8A investigations. In particular, the Tribunal said that “the examination by an employer of complaints of misconduct against staff is connected with the ‘administrative functions of an employer *qua* employer.’” These remarks do not sit well with the Tribunal’s view that disciplinary proceedings for medical misconduct amount to law enforcement, as discussed in the context of sections 23 and 24 above.

10.45 However, it is quite clear from the terms of the Act that the legislature intended that the IPPs should apply to the Police where they are exercising administrative or educative functions, but not otherwise. In the event that,

- the Police were bound by the IPPs with respect to their internal disciplinary investigations; and
- the Part 8A exemption from the definition of personal information did not apply;

an amendment in line with Recommendation 19 should address their concerns. No further amendment is therefore proposed.

APPLICATION OF THE IPPS AND EXEMPTIONS TO THE IPPS

10.46 The Privacy Commissioner is clearly of the view that the IPPs and exemptions to them do not act to authorise conduct by agencies that is otherwise specifically prohibited by another Act.

10.47 The Privacy Commissioner has suggested that a clarifying amendment to the Act be considered so that:

- the IPPs do not authorise any conduct that would be prohibited under any other law, contract or obligation, except where explicitly stated in the Act; and
- the exemptions to the IPPs (in the Act, a Regulation, a code of practice or a section 41 Direction) only modify the application of the IPPs and do not authorise any conduct that would be prohibited under any other law, contract or obligation.

10.48 Such an amendment would clarify that Privacy Act, and instruments made under it, are not able to override other Acts. As there is nothing in the stated objectives of the Act to suggest that the parliament intended this, the amendment is warranted.

⁴¹ *KO & anor v Commissioner of Police, New South Wales Police* (GD) [2004] NSWADTAP21

Recommendation 20

The Privacy Act should be amended so that it is clear that it cannot override the provisions of agencies' own operational statutes, which apply to regulate the management of personal information held by the agency.

CHAPTER 11

THE USE OF OTHER STATUTORY INSTRUMENTS TO MODIFY THE INFORMATION PROTECTION PRINCIPLES.

11.1 Section 20 (1) and (2) of the Act applies the IPPs to public sector agencies and provides that the application of the principles may be modified by privacy codes of practice.

11.2 Without the ability to modify the principles by making codes or relying on other exemptions in the Act some agencies would find that some of their day-to-day operations would not comply with the Act. Many agencies expressed frustration with the efforts required to ensure codes or section 41 directions were made and kept up-to-date although the ability to modify the Act in this way was not challenged. Other respondents were of the view that the Act was not transparent, creating an illusion of privacy protection, which is not delivered when the exemptions are considered.

REGULATIONS

11.3 Section 71 of the Act provides a very broad regulation-making power.

11.4 It specifically provides that regulations may make provision for or with respect to:

- the manner in which privacy codes of practice are to be prepared and developed; and
- exempting specified persons or public sector agencies, or classes of persons or public sector agencies from
- any of the requirements of the Act or the regulations relating to the collection, use or disclosure of specified classes of personal information; or
- any other provision of this Act.

11.5 To date the full scope of this power does not appear to have been explored, possibly because of the other methods available to agencies for modifying the IPPs. Regulations do not require consultation with, or approval of, the Privacy Commissioner but they are subject to possible disallowance by parliament. Parliamentary scrutiny has the advantage of creating transparency for the operation of the Act and also addresses what may be perceived as otherwise inappropriate delegation of legislative power to the Minister (in the case of codes) or the Privacy Commissioner (in the case of section 41 directions).

PRIVACY CODES OF PRACTICE

11.6 Part 3, Division 1 of the Act governs the making and operation of privacy codes of practice. Section 29 provides that, among other things, codes may:

- be made to protect the privacy of individuals; and
- regulate the collection, use and disclosure of, and the procedures for dealing with, personal information held by public sector agencies.

11.7 Codes can apply to:

- a specified class of personal information;
- a specified agency or class of agency;
- a specified activity or class of activity.

11.8 Although codes may modify the application of the IPPs or the public register provisions, they cannot impose more stringent standards than those set out in the IPPs. There is an inherent policy conflict in making codes that are to be made for the privacy protection of individuals (section 29) when they can only diminish the privacy protections in the IPPs (section 30).

11.9 Codes are made by an order of the Attorney General published in the Government Gazette. Before a code is made, consultation with the Privacy Commissioner is necessary. Any public sector agency or the Privacy Commissioner can initiate the drafting of a code. The Privacy Commissioner has published (on the PrivacyNSW website) a protocol for assessing draft codes of practice.

11.10 In order to introduce some uniformity into the drafting of codes the Parliamentary Counsel now drafts all codes. For easier access they are published as subordinate statutory instruments on the NSW Legislation website. However this process is relatively recent and all but two of the current codes are still in old formats and, in some cases, are only published in the Government Gazette. Ease of public access to these earlier codes is not as good as it should be and, in at least one case, has led to an application in the ADT in relation to conduct that was, unknown to the parties, governed by a relevant code.

11.11 There are currently 11 codes in place and a number being drafted. Generally, codes have been used to 'fill in the gaps' in exemptions to the IPPs that would otherwise restrict an agency's management of certain personal information.

11.12 Most of the codes that have been made to date relate to a single agency's conduct. The making of generic, cross-agency codes to govern the use of personal information in areas such as research, investigations, inter-agency transfers of information, ministerial correspondence and the like, has not been successful. Negotiations on draft codes in such areas have failed due to the inability of the process to meet the diverse interests of all agencies and to accommodate the Privacy Commissioner's brief (see section 36) to promote the adoption of, and assist agencies to comply with, the information protection principles. It is notable that where there is a common policy direction for the agencies negotiating the drafting of a cross-sector code and there is an overriding public interest in exempting agencies from certain privacy principles, there appears to be more likelihood of a code being made.

SECTION 41 DIRECTIONS

11.13 Section 41 provides that the Privacy Commissioner may make a written direction that:

- a public sector agency is not required to comply with an IPP or a code; or
- an IPP or code is modified as specified.

11.14 The Privacy Commissioner makes section 41 directions (called ‘public interest directions’ by the Commissioner). The Commissioner must be satisfied that the public interest in requiring an agency to comply with an IPP or code is outweighed by the public interest in making the direction. The Attorney General must approve the direction before it is made.

11.15 Section 41 directions have tended to be used by agencies and the Privacy Commissioner as a short-term solution to situations where agencies have an immediate need to carry out activities which would otherwise breach either the IPPs or a relevant code. They are relied on by agencies in order to carry out their core functions without breaching the Privacy Act. Of key importance to a number of agencies are the directions on:

- Indirect collection from third parties by human service agencies;
- Collection and disclosure for research purposes;
- The use of information for investigative agencies; and
- Some information transfers between public sector agencies.

11.16 The main problem with the use of section 41 directions is that what should be a short-term solution to an information management problem becomes the effective long-term solution. The directions are simply re-made continuously as they expire because of lack of satisfactory progress on negotiating a more long-term solution (usually a code). An examination of the directions currently in place shows that most current directions are now about four years old.

11.17 Many respondents want to see the proliferation of exemptions, caused by the various methods by which they can be effected, condensed into a more manageable and transparent regime. A number of respondents mention that the lack of a requirement for formal publication of directions (especially expired ones) makes accessibility an issue.

11.18 Noting that the Victorian Privacy Commissioner has no power to issue exemptions, and the Commonwealth Privacy Commissioner can only make public interest determinations after a lengthy consultation and hearing process, the Privacy Commissioner submits that the solution to these difficulties is:

- for agencies to rely on the broad exemption in section 25 of the Privacy Act and seek their own legislative authority for any conduct that would contravene the IPPs or public register provisions;
- to remove the code-making power;

- to proscribe the making of regulations that modify the IPPs and public register provisions;
- to codify, in the Act, the more long-term exemptions that exist in section 41 directions. The Commissioner singles out the exemptions for research and investigations that currently exist in section 41 directions for codification, as has been done in the Health Privacy Act;
- to provide a mechanism for the provision of binding statutory guidelines, made by the Privacy Commissioner, like that in the Health Privacy Act; and
- to preserve a more restrictive power for the Privacy Commissioner to make temporary directions (no more than 12 months) for exemptions with respect to both IPPs and the public register provisions and including the ability to affect classes of agency.

11.19 Some respondents, including the Privacy Commissioner, are keen for some form of section 41 direction to be retained on the basis that scope to modify the IPPs or a code on an urgent basis is required, although no examples were provided. Nor has it been suggested that the regulation making power could not be used in an urgent situation, if one ever arose.

11.20 Subsequent to his written submission, the Privacy Commissioner suggested that provision for section 41 directions be retained but that they be made the subject of a parliamentary disallowance motion by much the same procedure that exists for regulations.

11.21 The exemption process could be simplified by:

- removing the code making power;
- codifying, in the Act existing long term codes and directions; and
- making more extensive use of the regulation-making power and including a clear requirement to consult with Privacy Commissioner prior to making a regulation.

11.22 A more extensive use of the regulation-making power, which is subject to parliamentary scrutiny, has the benefit of affording the process far more public transparency. The issue of whether it is appropriate for regulations to be made which exempt agencies from adherence to the principles or public register provisions will then be able to be debated by the parliament, if necessary. As an advocate for privacy protection, giving the Privacy Commissioner an equivalent power to make urgent directions to derogate from privacy principles in the pursuit of another, stronger public interest may put the Commissioner in a difficult policy position. It is preferable for the Minister, who must weigh the competing public interests in maintaining or derogating from statutory privacy rights, to make such decisions.

11.23 If warranted, regulations can be and are made on an urgent basis. The Privacy Commissioner's role in providing expert advice on privacy can be maintained by following the regulatory process set out in the Subordinate Legislation Act. To guarantee that the Privacy Commissioner is not excluded from any role in the process, a statutory obligation to consult with the Commissioner prior to making a regulation could be created.

Recommendation 21

Exemptions in existing codes and directions should be reviewed and, where necessary, included in the Act or Regulations. Future variations to the application of the Act should be by way of Regulation only. Consultation with the Privacy Commissioner prior to the making of a regulation should be explicitly provided for.

GUIDELINES***Mass data matching***

11.24 Requests for mass data-matching are sometimes made of government agencies. The Privacy Commissioner gives the example of the Roads and Traffic Authority being asked to provide all drivers' odometer readings to the Office of Fair Trading, to assist the OFT in finding evidence of tampering.

11.25 A number of respondents, including the Privacy Commissioner have raised the issue of the need to manage mass data-matching projects conducted between public sector agencies in a more targeted way than the IPPs do presently.

11.26 The Privacy Commissioner suggests that he should be empowered to develop binding guidelines, based on balancing the relative public interest merits of the data-matching, to enable agencies that comply with the guidelines to use information collected for one purpose for a different purpose altogether. Provided that the guidelines were met, data matching of some kinds would be permitted where it is in the public interest.

11.27 The Privacy Act provides that the Commissioner may issue guidelines relating to the protection of personal information and other privacy matters. Introducing binding guidelines as another method by which exemptions to the application of the IPPs could be achieved is undesirable.

11.28 The Commissioner should exercise the existing power to issue guidelines. If it becomes evident that this power is insufficient, then the issue may be reconsidered.

CHAPTER 12

PUBLIC REGISTERS

12.1 Part 6 of the Act provides special rules in relation to the personal information held in public registers administered by the NSW public sector. Peculiar to this Part of the Act, it prevails over any requirements of the law under which the public register was established.

12.2 Section 57 of the Act says that before disclosing personal information held on a public register an agency must satisfy itself that “it is to be used for purpose relating to the purpose of the register or the Act under which the register is kept”. Agencies are authorised to request a statutory declaration from the user as to the intended use of the material disclosed.

12.3 The *Privacy and Personal Information Protection Regulation 2000* exempts a number of public registers from the provisions of Part 6.⁴² Other public registers relating to environmental protection initiatives and the majority of health professionals⁴³ are exempt from Part 6 by virtue of the Privacy Code of Practice (General) 2003.

12.4 Respondents that administer public registers commonly submitted that the provisions (without modification) are unworkable in practice. In particular, in circumstances where it is desirable (usually for reasons of accountability and accessibility) for the public register to be given a wide circulation by, for instance, publication on the internet, the requirement that the agency be satisfied the information will be used for a purpose relating to the purpose of the register acts to prevent such publication even if a person consents to it. Another respondent queries the need for regulation of public registers, since their purpose is to provide information to the public. By exempting them from the provisions of the Part, the Regulation and the code provisions detailed above have addressed these issues with respect to the key public registers covered.

12.5 The Privacy Commissioner expresses concern about the fact that if a public register is published on the internet, it may be possible for the home address of a doctor, or the name of the owner of a particular property to be obtained and used by people with no legitimate right to know this information or, even worse, who may use the information to harm the person in some way. The Commissioner suggests that the public register provisions need to be repealed and that the information be dealt with

42 That is: the Torrens Register and any Index maintained under the Real Property Act 1900; the General Register of Deeds maintained under s 184C of the Conveyancing Act 1919; any Index kept under section 198 of the Conveyancing Act 1919; the Central Register of Restrictions maintained under Part 24 of the Conveyancing Act 1919; the Register of Land Values kept under the Valuation of Land Act 1916; the register of justices of the peace kept under the Justices of the Peace Act 2002 and the Water Access Licence Register kept under section 71 of the Water Management Act 2000. The Councils of the Law Society and the Bar Association in NSW (which maintain registers of practitioners) are exempt from all the provisions of the Act.

43 Including doctors, nurses, dentists, dental technicians, optometrists, optical dispensers, osteopaths, pharmacists, podiatrists, psychologists, chiropractors and physiotherapists.

under the IPPs concerning disclosure (with suitable amendments) and by the provision of 'reasonably necessary'-type exemption. The Commissioner envisages a provision that would generally prohibit widespread publication on the Internet in the absence of specific legislative authority to publish the information at large.

12.6 Notwithstanding the Privacy Commissioner's concerns about the potential dangers of publishing public registers on the internet this did not emerge as a particular concern of other respondents, even though a number of significant public registers have been put beyond the reach of the Act.

12.7 Section 58 allows for suppression of personal information held on a public register. The test for suppression is multi-layered. It compels an agency to suppress information as requested

- if it is satisfied that the safety or well-being of any person would be affected by not suppressing the information; and
- unless the public interest in maintaining public access to the information outweighs any individual interest in suppression.

12.8 Although the Privacy Commissioner submitted that the provision is difficult to apply, it was not the subject of specific comment by agency respondents.

12.9 It is notable that the Privacy Commissioner has supported the exemption of a number of public registers from the ambit of the Act. In this context it should be noted that once the Privacy Act does not cover a particular public register, it can be regulated by the terms of the Act under which it is created. Representations made by the Privacy Commissioner may influence policy decisions about such regulation. Otherwise section 59 of the Act applies so that Part 6 prevails, to the extent of any inconsistency with the requirements of the law under which the public register was created.

12.10 At this time there does not seem to be sufficient justification for amendment of the Act as suggested by the Privacy Commissioner. It appears that the terms of the Act as they relate to public registers and modifications to their application are working as parliament intended.

CHAPTER 13

ROLE OF THE PRIVACY COMMISSIONER

FUNCTIONS

13.1 The functions of the Privacy Commissioner are set out in the Privacy Act and include:

- providing assistance to agencies in compliance with the IPPs and codes of practice, including the preparation and implementation of privacy management plans;
- preparing guidelines and promoting their adoption; and
- education, research and publication functions, including the making of public statements; and
- complaint handling and review, including the ability to make special reports to parliament.

13.2 Even though the Commissioner's functions include the function of recommending legislative and administrative change or other action in the interest of the privacy of individuals (section 36(2)(j)) the Commissioner submits that his role in government policy making requires further refinement. In particular, he suggests that consideration should be given to:

- requiring all government proposals to include a Privacy Impact Assessment which investigates and considers the impact of the proposal on privacy protection;
- adopting a provision like that in the Victorian Information Privacy Act, which gives the Victorian Privacy Commissioner a statutory function to advise the Attorney General on any legislative proposal that may interfere with, or have an adverse impact on privacy.

13.3 Most agencies seem comfortable with preparing and implementing their own privacy management plans. Some make positive comments about the Privacy Training CD prepared by Privacy NSW in this context.

13.4 However, the issue of resources for the Privacy Commissioner's office was the subject of comment by a number of respondents. The Commissioner feels he is limited in his ability to fulfil all of his functions. At the same time some agencies would prefer more timely and effective assistance from the Commissioner.

13.5 Although these are real issues in the administration of privacy protection, it is beyond the scope of a review of the Act to investigate the funding decisions of government.

13.6 Introducing Privacy Impact Assessments may have the effect of sharing the load relating to privacy protection across the whole of government. However, to make these mandatory, or to introduce an obligation to consult with the Privacy

Commissioner on all legislative proposals that may impact on privacy, derogates from the right of executive government to determine how to develop government policy and goes beyond the current terms of the Privacy Act. Since the current functions of the Commissioner give broad scope to influence privacy policy, expansion of those functions is not warranted at this time.

13.7 In the face of the relatively low number of complaints dealt with by the Commissioner,⁴⁴ a more targeted use of the available funding by the Privacy Commissioner may be warranted. A stronger focus on the provision of public education and constructive guidance to public sector agencies could produce a more compliant public sector, a more privacy-aware community, and even fewer complaints.

A 'STAND-ALONE' PRIVACY COMMISSIONER

13.8 A number of respondents raised the issue of whether a 'stand-alone' Privacy Commissioner was the best way of delivering privacy rights to aggrieved citizens, or whether a new model for delivery of the services associated with the rights set out in the Act should be considered.

13.9 Such concerns were often expressed in the context of perceived conflicts between rights under the Freedom of Information Act (which are managed by the Ombudsman) and the Privacy Act (managed by the Privacy Commissioner). In this context the Access to Information Inquiry⁴⁵ has previously explored a number of different models for managing privacy and information protection in common law countries. In other jurisdictions with legislative privacy and/or freedom of information protections, they are overseen in various combinations. Variations include separate FOI and privacy commissioners with separate Acts to administer or a single 'information' commissioner, administering either a single Act covering both information privacy and access to information regimes or separate Acts for each regime.

13.10 In the *Privacy Amendment Bill 2003*, the government indicated a preference for the transfer of the functions of the Privacy Commissioner to the Ombudsman, while retaining a separate statute governing privacy.

13.11 In the context of this review a range of proposals for the future oversight of privacy protection in NSW were put forward including:

- Revision of the Privacy Act to allow one office to manage both FOI and privacy matters; and
- If responsibilities for privacy and freedom of information are to be more closely aligned, then either:
 - a single information commissioner should be created; or
 - the Privacy Commissioner's responsibilities should be transferred to the Ombudsman.

⁴⁴ see the analysis of operations of the Privacy Commissioner in Chapter 3 of this Report.

⁴⁵ NSW Parliament, op cit.

13.12 There is an inherent policy dilemma in merging a regime predicated on a citizen's right to transparency in government (freedom of information) and a regime which is concerned with protecting the individual's right to having their personal information protected by government (privacy).

13.13 The central policy issue arising from the question of whether a dedicated Privacy Commissioner is preferable to an administrator with responsibility for the management of all information about citizens held by government is which alternative better protects the privacy of individuals.

13.14 In theory, a 'stand-alone' Privacy Commissioner may be best placed to avoid this policy dilemma. On the other hand, combining rather than dividing the resources devoted to information management (privacy and FOI) may ensure privacy is placed on a more equal footing (in terms of resources) with FOI than is presently the case.

CHAPTER 14

COMPLAINT AND REVIEW MECHANISMS

INTRODUCTION

14.1 While a number of respondents noted the limits of privacy protection that is predicated on rules (IPPs) that may be enforced by a system of administrative review, these views overstate the limitations of the privacy protection available in NSW.

14.2 In fact the Privacy Commissioner, somewhat unusually for statutory privacy regimes in Australia, has broad powers of:

- inquiry and investigation (with the powers, authorities, protections and immunities accorded a Royal Commissioner);⁴⁶
- conciliation; and
- reporting (including special reports to parliament)⁴⁷ on any matter pertaining to the protection of the privacy of individuals.

14.3 These powers extend to privacy rights beyond the obligations of public sector agencies to adhere to the IPPs set out in the Act.

14.4 The Commissioner's complaints experience under the Act is analysed in the Annual Reports of Privacy NSW. An overview of the reports up to the 2002-2003 reporting year, in relation to complaints, can be found in Chapter 3 of this Report. Perhaps because of the extent of the complaint handling powers, there may have been an over emphasis on managing complaints on the part of the Privacy Commissioner.

14.5 It should be noted that despite these relatively extensive powers, the number of complaints to the Privacy Commissioner's Office is relatively small when compared with the size of the public sector, and the community generally. Considering the fact that the ADT has found a contravention of the Act by a public sector agency in only seven matters since its jurisdiction commenced in 2000 and that in only one of the seven was the conduct set aside, there seems to be justification for a greater focus on the educative and advice functions of the Commissioner. It is against this background that the complaint and review mechanisms are reviewed.

COMPLAINTS

14.6 The protection of the privacy of individuals generally is accomplished by the application of the rules set out in Part 4, Division 3 of the Act. Sections 45 to 51 set out the Privacy Commissioner's complaint handling powers; including an obligation, under section 49, to endeavour to resolve a complaint by conciliation. The Commissioner has powers to compel a person to appear before him or her in

⁴⁶ *Privacy Act*, s.38.

⁴⁷ *Privacy Act*, s.65.

conciliation proceedings and to make a report on findings or recommendations in relation to a complaint.

14.7 Under these rules the Privacy Commissioner may investigate any complaint about an alleged violation of or interference with the privacy of an individual. This broad power means that the Commissioner can (and does) investigate complaints that go beyond the conduct of NSW public sector agencies and a breach of the IPPs.

14.8 This complaints process is usually used for assessing complaints of breaches of privacy that do not come within the framework of protection afforded personal information held by the public sector. The Privacy Commissioner has established policies on the management of these matters. It is distinct from an applicant's entitlement to internal and external review of the conduct of public sector agencies provided for in Part 5 of the Act. While there are no enforceable remedies available to applicants seeking to complain to the Commissioner pursuant to section 45, applicants for review may seek remedies including apologies, monetary compensation and the like.

14.9 Although one respondent suggested that the ability of the Commissioner to investigate complaints about the privacy of an individual that is not otherwise protected by the Act should be abolished, this was not a commonly held view.

14.10 The Privacy Commissioner has made many recommendations for reform relating to the complaints processes provided for in the Act. A primary concern is the focus on the individual complainant, rather than giving scope for the investigation and resolution of systemic privacy issues. Although not many other respondents share these concerns the President of the ADT (formerly a Commonwealth Privacy Commissioner) draws attention to the successes of the Commonwealth conciliation based/commissioner determination model of managing privacy complaints, particularly in addressing systemic issues, and in establishing a cooperative relationship with public sector agencies.

14.11 The President nominates several important factors as contributing to the success of this model at the Commonwealth level including:

- The use of manuals and guidelines to give specific direction and advice to public sector staff in the operation of the IPPs (but without the status of legal regimes);
- The power of the Commissioner to make final determinations, (even though it is rarely used);
- The strict specialisation in privacy matters permitted by the model;
- The use of experienced investigative staff, who had credibility with agencies, developed by dealing neutrally and impartially with complainants and agencies, and whose fact finding was of a high quality; and
- The Commissioner's office operating a fully developed inquisitorial model of complaint resolution.

14.12 This assessment of the success of the Commonwealth model of complaints handling suggests that perceptions of success or failure in this area may depend more

on the development of a culture of regulation by cooperation rather than on detailed legislative authority.

14.13 In comparison to the ‘commissioner determination’ model, the Privacy Act allows an applicant to seek investigation/conciliation by the Commissioner and then go to the ADT, although the six-month time limit for internal review⁴⁸ acts as a natural barrier to this and other informal attempts to resolve prospective applicants privacy concerns. In practice, complaints about breaches of the IPPs, codes and public register provisions of the Act are usually managed in accordance with Part 5 of the Act, so that the Privacy Commissioner does not occupy a central role in this process.

14.14 Some respondents, notably the larger service delivery agencies, felt that more scope for informal negotiations about privacy complaints made to public sector agencies is warranted.

14.15 Conversely, the NSW Privacy Commissioner suggests that some of the problems with his complaints and investigations powers could be resolved by greater legislative powers, such as:

- explicitly providing for complaints by third parties, such as whistleblowers and representative/class action type complaints;
- specifying what findings the Commissioner can make pursuant to section 45 (1) and section 50. In particular; that the Commissioner can reach findings as to breaches of the IPPs or other applicable standards, in determining whether or not there has been a ‘violation of, or interference with’ a person’s privacy; and
- more precision in the Act about the process of investigating and conciliating complaints, including:
- when to decline a complaint; and
- a power to conduct ‘own-motion’ investigations and investigate complaints even where the complaint is withdrawn or the complainant is anonymous.

14.16 Overall, there is no clear need for an expansion of the Privacy Commissioner’s complaint-handling role made out in the submissions, and no suggestion that the terms of the Act have failed to achieve the legislature’s objectives of providing for the making of complaints about privacy related matters. In fact, to adopt the suggestions of the Privacy Commissioner in this area may have the effect of further concentrating the Privacy Commissioner’s resources in complaints handling, at the expense of bolstering the Commissioner’s focus on education and advice.

14.17 Some submissions suggested that the Privacy Commissioner’s investigation decisions should be reviewable in the ADT. The Commissioner asserts that giving the ADT such a role would place him in an untenable position vis-à-vis his role in appearing before the ADT in matters that have been the subject of internal review by public sector agencies. As it is conceivable that some complainants choose to have the Commissioner investigate a complaint in order to maintain confidentiality,

⁴⁸ See further discussion of the time limit for internal review at page 66 below.

because they seek a more informal process, or to avoid victimisation,⁴⁹ it is not proposed to subject the Commissioner's investigation decisions to review at this time. In the event that it becomes obvious that some external scrutiny of the Commissioner's investigations is necessary for reasons of public accountability, the matter may be revisited.

Recommendation 22

The Privacy Commissioner should be encouraged to continue to develop effective partnerships with the community and the public sector in developing strategies to better protect the privacy of individuals and adopt best practice strategies (based on the IPPs) for the protection of personal information.

ADMINISTRATIVE REVIEW

14.18 A person aggrieved by the conduct of a public sector agency is entitled to elect to have the complaint dealt with by the Commissioner in accordance with Part 4, Division 3, or under Part 5.

14.19 Part 5 (concerning administrative review) applies to conduct by a public sector agency that is alleged to be in contravention of the IPPs, a privacy code of practice or the disclosure of personal information kept on a public register. It provides for internal review by the agency, and external review by the ADT.

14.20 The Commissioner points out that section 52 of the Act (although expressed differently) applies to conduct which is either non-compliance with an IPP or non-compliance with the public register provisions. The reference to codes of practice is confusing in this context, as their operative parts only ever derogate from the rules set out in the IPPs. Furthermore, if Recommendation 21 is accepted, the reference to codes will become superfluous.

Recommendation 23

Section 52 should be clarified to apply to conduct that is non-compliant with an IPP or the public register provisions.

INTERNAL REVIEW

14.21 Section 53 gives an aggrieved person a right of internal review by the agency whose conduct is complained of. The agency reviewer, who should not be associated with the conduct complained of, is bound to notify the Privacy Commissioner of the complaint and keep the Commissioner informed of the progress and findings of the review.

14.22 The reviewer is required to take into account relevant material put to him or her by the aggrieved person and the Privacy Commissioner. As a matter of practice the Commissioner has usually restricted himself to advising on procedural matters and or 'best practice' for internal reviews, and has issued a checklist for agencies to follow. Concern about a potential conflict of interest if subsequently required to

⁴⁹ See further discussion about victimisation at page 70.

appear before the Tribunal is the basis for this approach. An agency may ask the Privacy Commissioner to conduct an internal review on its behalf, although the Commissioner has not accepted this role either, because of a perception that potential for a conflict of interest is too great.

14.23 Generally, agencies do not have major concerns about their management of internal reviews. While the Commissioner makes a number of suggestions for legislative clarification of the internal review process, he also acknowledges in the submission that the more recent internal review reports reveal that agencies are doing a better job than they were initially in the conduct of these reviews.

Who can conduct internal reviews?

14.24 The Commissioner does, however, suggest that internal review would work better for some agencies if each agency appointed an officer as its privacy contact officer, who would be the main point for liaison with the Commissioner and whose role would include the co-ordination of internal reviews. However, many agencies already have designated privacy officers. In the absence of significant public concern, these matters are generally best addressed by agencies' own management structures. Of more consequence is the Commissioner's submission that it is sometimes difficult for smaller agencies to find an appropriate person within the agency to conduct the review, and that an ability to out-source this work would be useful.

Recommendation 24

Agencies should be able to out-source their internal review obligations to appropriately qualified agents.

'Person aggrieved'

14.25 The Privacy Commissioner has noted that a 'person aggrieved' in internal review⁵⁰ is a wider concept than 'person whose personal information is in issue', and suggests that it be clarified to support 'representative' claims. Representative claims have been used in the Commonwealth environment to resolve complaints about tenancy blacklists. While this type of matter would not be within the administrative review jurisdiction of the NSW Act, it may be useful in resolving systemic issues relating to an agency's management of a particular type of information in, for instance, mass data-matching projects.

14.26 The general law tends to support the conclusion that 'person aggrieved' is a wider class than an individual whose personal information is in issue. Although the ADT has found that an applicant was aggrieved because he had been specifically and adversely affected by an alleged breach of the Act involving the personal information of his son⁵¹ the extent of the class, in the context of the Privacy Act, has not yet been fully tested.

⁵⁰ *Privacy Act*, s.53 provides that 'A person...who is aggrieved by the conduct of a public sector agency, is ...entitled to a review of that conduct. Pursuant to section 55(1) a person who has made an application for internal review under section 53 (and) is not satisfied ... may apply to the (ADT) for a review of the conduct that was the subject of the (s 53) application.'

⁵¹ *KO & Anor v Commissioner of Police, NSW Police* [2004] NSWADT 208.

14.27 Taking into account the concept of ‘aggrieved person’ in the general law, the legislature has provided for the possibility of an applicant for review being someone other than the person immediately affected by an agency’s conduct. The ADT has interpreted the provision in this light. Accordingly, there is no need to adopt the Privacy Commissioner’s suggestion at this time.

Time limits for internal review

14.28 A person who is aggrieved by the conduct of a public sector agency must lodge an application for internal review of the conduct by agency within six months of becoming aware of the conduct (or such later date as the agency may allow).

14.29 The ADT has decided⁵² that an agency’s discretion whether or not to accept applications for internal review out of time (that is, after the six months allowed in section 53(3) of the Act) is non-reviewable. It was submitted by two respondents that the non-reviewable discretion could potentially disadvantage applicants who first seek to resolve the matter informally. It was suggested that a more flexible approach to the six month time limit could be adopted. On balance, however, six months is regarded as a reasonable time period within which to lodge an internal review. Further, it is appropriate for an agency’s discretion regarding whether or not to accept applications for internal review to remain non-reviewable in order to limit an agency’s exposure to a privacy complaint that is too old to be properly investigated.

Victimisation

14.30 Even though the issue was not generally canvassed in other submissions, the Privacy Commissioner is concerned about the potential for victimisation of an applicant for internal review, especially if they are an employee or contractor of the agency involved. The Commissioner says that it has been the experience of the Office that applicants who have the least trust in the agency or the most to lose (for instance, loss of employment or service provision or a contract) will be the least likely to choose administrative review, preferring instead an investigation by the Commissioner. However, the comparative figures for investigation/conciliation, compared to internal review in the 2002-2003 Annual Report of Privacy NSW do not support this assertion.⁵³ Accordingly, the need to provide special protections against victimisation, beyond the provision of a power for the Commissioner to conduct a non-reviewable investigation, has not been made out.

REVIEW IN THE ADT

Privacy Commissioner’s role

14.31 The Privacy Commissioner and some other respondents complain that applications before the Tribunal are one-sided affairs, with applicants who have no knowledge of the process or the law typically representing themselves against well-resourced agencies, with representatives who are familiar with the process and

52 in *Y v DET* [2001] NSWADT 149.

53 The Report indicates that there have been many more internal reviews (108) than complaints proceeding to investigation/conciliation (40), even though employees are the second most common category of applicant for both complaints and internal review.

arguments (often about statutory interpretation). Possibly with this power imbalance in mind, the Act provides for the Privacy Commissioner to take part in Tribunal proceedings. The ADT has found that the Commissioner should be given a comparable role before the Tribunal's Appeal Panel, even though it is not specifically set out in the Act. The President of the Tribunal has suggested that legislative clarification is warranted.

14.32 The effectiveness of the Privacy Commissioner's role in the Tribunal was not the subject of comment by respondents. However, the Privacy Commissioner is concerned that because some parties think that his role is to advocate on behalf of applicants, agencies may perceive the Office as biased and be reluctant to seek assistance from it in other contexts. Legislative guidance as to the scope of the Commissioner's role may alleviate this concern.

Recommendation 25

The Act should:

- set out the scope of the Privacy Commissioner's role in the ADT as determined in consultation with the Commissioner and the President of the Tribunal, but primarily to assist in matters of statutory interpretation and privacy practice in NSW; and
- clarify that the Commissioner may appear in privacy matters before the ADT Appeal Panel.

A time limit for applications

14.33 The Privacy Commissioner and the ADT noted that there is no time limit for lodging privacy applications in the Tribunal. This is an unreasonable burden for agencies and should be rectified. The Commissioner and the Tribunal agree that applications to the Tribunal should be made within 60 days of an applicant being advised of the outcome of an internal review.

Recommendation 26

Applicants should be allowed 60 days from the date of completion of an internal review to file an application for external review in the ADT.

Original or review jurisdiction?

14.34 The ADT's jurisdiction is divided conceptually into 'review of reviewable decisions' and original decision making. Privacy Act matters are cast as 'review of reviewable conduct' and the Tribunal is required to make an original decision about that conduct.

14.35 Whether or not the Tribunal's jurisdiction is classified as review or original makes a difference because it affects what powers it has under the ADT Act. The ADT has found that it hears privacy matters in its review jurisdiction⁵⁴ but submits that there is a need for clarification of this point.

14.36 It should be noted that in the Health Privacy Act the ADT's jurisdiction is cast as original.

Recommendation 27

The Act should make clear that privacy matters are heard in the ADT's review jurisdiction.

Remedies

14.37 The Privacy Act makes provision for the payment of monetary compensation. Before ordering monetary compensation the Tribunal must be satisfied that the conduct caused certain sorts of harm, specifically: financial loss, or physical or psychological harm.

14.38 The Department of Housing wanted to see this further refined so that compensation is only payable if there is actual economic loss or diagnosed psychiatric injury. No other submissions suggest that this kind of limitation should be considered.

14.39 Another respondent complained about the exclusion of prisoners and their family and friends from the right to financial compensation.

14.40 The Privacy Commissioner noted that the available remedies make it difficult for the Tribunal to make orders to deal with systemic problems that are evident from an individual complaint. It is however open to the Privacy Commissioner to use his educative and advisory functions to assist agencies if decisions of the Tribunal suggest that there is a systemic issue that needs addressing. If the matter is intractable, then the use of the Commissioner's powers to make a special report to parliament or make recommendations to the relevant minister may be appropriate.

⁵⁴ see *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132

CHAPTER 15

MISCELLANEOUS MATTERS

PRIVACY MANAGEMENT PLANS, ANNUAL REPORTING REQUIREMENTS FOR AGENCIES AND PERSONAL INFORMATION DIGESTS.

15.1 Section 33 of the Privacy Act requires all public sector agencies to have a privacy management plan. The plan must include policies and practices to ensure compliance with the Act and strategies for disseminating them to staff. An up-to-date copy is to be provided to the Privacy Commissioner.

15.2 Section 33 also obliges all agencies to report on their compliance with the Privacy Act in their annual report.

15.3 Section 40 provides that the Privacy Commissioner “may, from time to time, prepare and publish a personal information digest setting out the nature and source of personal information held by public sector agencies.” and that the Privacy Commissioner can compel agencies to provide him with the information he requires to prepare this report.

15.4 Most respondents had nothing, or nothing negative, to say about provisions in the Act that require agencies to furnish the Privacy Commissioner with details relating to personal information they hold. Similarly, agency respondents did not seem concerned about the obligations they have to prepare and maintain privacy management plans and report annually on compliance with the Privacy Act.

15.5 The Privacy Commissioner expressed the view that the storage of management plans is problematic for that Office and that the documents are not necessarily helpful to an individual seeking to assert their privacy rights. However, a central database of the plans should go some way to ensuring access for staff and members of the public.

15.6 The Commissioner also expressed the view that the annual reporting requirements are of little practical effect in their present form. However, requiring agencies to give details of their compliance with the Privacy Act in their annual report means that agencies’ attention is drawn to privacy issues at least on an annual basis. If there are indications that an agency or agencies are experiencing difficulty in managing their privacy obligations, there is nothing to preclude the Commissioner from suggesting that the agency’s privacy management plan be revised.

CHAPTER 16

CONCLUSION

16.1 Most public sector agencies appear to take their obligations under the Privacy Act seriously, with many using the IPPs as the guiding principles for the management of personal information. Thus parliament's intention to provide for the protection of an individual's privacy in the public sector by requiring agencies to turn their mind to how they manage the personal information they hold has been achieved. In this context, it is noteworthy that when comparing the size and make up of the public sector⁵⁵ in 2003 with the number of complaints that proceeded to conciliation⁵⁶, internal reviews⁵⁷ and external review⁵⁸, the conclusion may be drawn that citizens are generally satisfied with the way in their privacy is protected by the Act. It may be concluded from this that:

- agencies are getting better at the conduct of internal reviews (as confirmed by the Privacy Commissioner);
- ADT decisions are assisting agencies to better understand their obligations under the Act; and
- management of personal information in the public sector is improving.

16.2 The fact that most agencies think that the Act's objectives have been achieved indicates that, to some extent at least, it has been effective in this regard. The keen participation of agencies in this review suggests that generally speaking, they are concerned to ensure that the privacy rights of the individuals who are their clients are considered in the delivery of government services.

16.3 Nevertheless, there was widespread dissatisfaction with the way in which the Act operates in practice and many suggestions for reform. The nature of the dissatisfaction ranges across the entire Act, with the emphasis differing between respondents according to their interests. In particular, most public sector agencies were very concerned to point out operational deficiencies in the Act. Thus the recommendations in this report concerning the operation of the information protection principles focus on clarifying their operation and methods of modifying their application, rather than suggesting a more rigorous application of the principles to agencies.

16.4 In the context of the IPPs concerning access and maintenance of records, many agencies reported concern about the interaction between the operation of the Privacy Act and Freedom of Information Act, and the State Records Act. Particular concerns were also expressed in the local government sector about the application of the Local Government Act rules about access to information. While these issues have also been raised in the context of the Access to Information Inquiry being conducted

55 344,000 employees in 2003, 72% of whom were employed in the health education and public order and safety sectors.

56 40 in 2003.

57 108 in 2003.

58 38 in 2003.

by the Parliamentary Committee on the Office of the Ombudsman and the Police Integrity Commission it is clear, when the Committee's deliberations to date are considered, that most agencies would prefer one set of rules regulating the access and alteration of information they hold. A recommendation to this effect is made in this Report.

16.5 The effectiveness of a separate office of the Privacy Commissioner was raised in both the context of the application of FOI and state records legislation, as well in relation to the adequate resourcing of the Office. While there are several differing models for the administration of privacy and other access to information regimes in other jurisdictions, there does not appear to be an overwhelming case in favour of a model other than that set out in the existing Privacy Act.

16.6 The oversight of public sector agencies' adherence to the IPPs by the process of internal review and external review to the ADT, whilst criticised by some as often being a one-sided contest in favour of agencies, did not attract significant adverse comment. Again, while there were some advocates for the adoption of a different model for the oversight of privacy, there was no overwhelming case made out for reform of the model of administrative review, coupled with broad investigation and recommendation powers for the Privacy Commissioner set out in the Privacy Act. Greater cooperation between the office of the Privacy Commissioner and public sector will assist in achieving the twin objectives of effective service delivery by government agencies, and protection of the privacy of individuals.

16.7 The Privacy Commissioner's powers are not limited to applying the IPPs to the public sector. The Commissioner has extremely wide powers of inquiry and investigation, including the capacity to make recommendations and findings in respect of complaints about an alleged violation of or interference with the privacy of an individual. These powers give the Commissioner ample scope for achieving the objective of protecting the privacy rights of individuals, even though there is no strict method of enforcement in relation to these powers. Although the Privacy Commissioner made a number of submissions to improve the ability of the Office to manage complaints, in the context of these broad powers of investigation and reporting, they were usually unwarranted. Furthermore, to adopt these recommendations has the potential to refocus the Commissioner's energies on complaint handling, when it is clear that there needs to be a shift away from this aspect of the Commissioner's work and a greater emphasis placed on the research and education functions of the Office.

16.8 Finally, while the Act does appear to be meeting its objectives by providing a framework for privacy protection in NSW, there is significant scope for clarification of the extent of that protection. Appropriate amendments to the information protection principles, so that the circumstances of their application are more clearly set out, would assist the public sector and those who seek to enforce their privacy rights.

APPENDIX A

Respondents to the review

GOVERNMENT AGENCIES AND SOCS

1. Aboriginal Affairs, NSW Department of
2. Ageing, Disability and Home Care, Department of
3. Agriculture NSW
4. Arts, NSW Ministry of
5. Attorney General's Department (FOI/Privacy)
6. Australian Museum
7. Casino Control Authority NSW
8. Children and Young People, Commission for
9. Community Services, NSW Department of
10. Corrective Services, Department of
11. CountryEnergy
12. Education and Training, Department of
13. Energy Australia
14. Environment and Conservation, Department of
15. Fair Trading, Office of
16. Fisheries NSW
17. Health NSW
18. Housing, Department of
19. Infrastructure, Planning & Natural Resources, Department of
20. Institute of Sport NSW
21. Integral Energy
22. Juvenile Justice, Department of
23. Local Government, Department of
24. Police, Ministry of
25. Roads and Traffic Authority (RTA)
26. State Library of NSW
27. State Revenue, Office of
28. Sydney Olympic Park Authority
29. Sydney Ports Corporation
30. Waterways Authority
31. Women, Department of

STATUTORY AUTHORITIES

1. Charles Sturt University
2. Community Relations Commission
3. Community Relations Commission
4. NSW Parliament
5. Ombudsman NSW
6. Police Integrity Commission
7. Director of Public Prosecutions
8. Public Trustee NSW
9. University of Sydney

LOCAL COUNCILS

1. Bankstown Council
2. Baulkham Hills Council
3. Boorowa Council
4. Canterbury City Council
5. Coffs Harbour City Council -
6. Gosford City Council
7. Greater Queanbeyan City Council
8. Hawkesbury City Council
9. Hunter's Hill Council
10. Lismore City Council
11. Pittwater Council
12. Port Stephens Council
13. Randwick City Council
14. City of Sydney

HEADS OF JURISDICTION

- | | |
|--------------------------------------|------------------------|
| 1. Administrative Decisions Tribunal | Judge Kevin O'Connor |
| 2. Coal Compensation Board NSW | H N Bowman |
| 3. District Court of NSW | Hon Justice R O Blanch |

PRIVACY COMMISSIONERS

- | | |
|---|---|
| 1. PrivacyNSW, Acting Privacy Commissioner | |
| 1. Commonwealth Privacy Commissioner, Office of | - |
| 2. Privacy Victoria | |

INSTITUTIONAL STAKEHOLDERS

1. Australian Privacy Foundation
2. Australian Society of Archivists (NSW Branch)
3. Australian Society of Archivists
4. Governance Network Group
5. Intellectual Disability, NSW Council for
6. Kingsford Legal Centre
7. Public Interest Advocacy Centre
8. Timmins Consulting Australian Pty Ltd

MEMBERS OF THE PUBLIC

1. Max Eastcott-Layton
2. P A Gargan
3. KJ
4. Peter B McKell/I Notaras
5. Harold Shaw
6. W J Walsh

APPENDIX B

ADMINISTRATIVE DECISIONS TRIBUNAL – OUTCOMES IN APPLICATIONS PURSUANT TO THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT (AS AT 16 MAY 2005)

<i>Year</i>	<i>Total disposed</i>	<i>Decision affirmed</i>	<i>Settled / withdrawn / dismissed (no jurisdiction)</i>	<i>Contravention found but no action taken by Tribunal</i>	<i>Decision set aside</i>
2000/2001	1		1		
2001/2002	6	2	4		
2002/2003	22	3	19		
2003/2004	28	3	22	3	
2004/2005	34	7	23	3	1
2005/2006	0				