NSW LAW REFORM COMMISSION

Consultation Paper 3

Privacy Legislation in New South Wales

June 2008

New South Wales. Law Reform Commission.

Sydney 2008

ISSN 1834-6901 (Consultation paper)

National Library of Australia

Cataloguing-in-publication entry

Privacy Legislation in New South Wales.

Bibliography

ISBN 978-0-7347-2633-9

1. Privacy – Law and legislation – New South Wales. I. New South Wales. Law Reform Commission. (Series : Consultation paper (New South Wales Law Reform Commission) ; 3).

342.0858

Table of Contents

Terms of Reference viii
Participants ix
Submissions x
List of proposals and issues xi

1. Introduction

Putting this paper in context 2
ALRC'S review of privacy law 2
The purpose of this paper 4
Further issues 5
Information sharing 6
Criminal sanctions 7
An outline of the chapters 8

2. Current privacy protection - Commonwealth

Introduction 12
The *Privacy Act 1988* (Cth) 12
The Commonwealth Information Privacy Principles 13
The National Privacy Principles 14
A unified set of principles 15
Exceptions and exemptions 16
Breaches 17
Enforcement 18
Other federal privacy legislation 19

3. Current privacy protection - New South Wales

Introduction 22
The *Privacy and Personal Information Protection Act 1998* (NSW) 22
Background and development of PPIPA 23
What is covered? 24
What is "personal information"? 25
Who is covered? 26
The Information Protection Principles 27

Exemptions 29
Enforcement 32
The *Health Records and Information Privacy Act 2002* (NSW) 36
Historical background 36
What is covered? 38
The Health Privacy Principles 40
Consent 43
Exemptions 44
Other exemption mechanisms 45
Enforcement 45
Other related New South Wales legislation 47

4. Achieving a clear and consistent legislative structure

Introduction 50
Clarifying the structure of New South Wales privacy laws 51
The structure of PPIPA 51
The structure of HRIPA 53
Difficulties with the structure of PPIPA 54
Level of detail 55
The Commission's view 56
Should PPIPA have an objects clause? 58
The Commission's view 59
Achieving greater consistency in health information 60
Private sector coverage of health information under HRIPA 62
The Commission's view 63
Should health information continue to be regulated separately? .. 64

5. Scope of privacy protection

Introduction 68
Should the scope of PPIPA and HRIPA be expanded by reducing or limiting exemptions? 68
Background 68
Personal information – PPIPA s 4; HRIPA s 5 69

Definition of "public sector agency" - PPIPA s 3(1); HRIPA s 4(1) 85
Unsolicited information – PPIPA s 4(5); HRIPA s 10 86
Law enforcement and investigative agencies – PPIPA s 23, 24 and 27; HRIPA s 27 89
State owned corporations 92
Government contractors 95
Should other aspects of privacy be expressly protected in PPIPA? 96
Background 96
What are "privacy related matters"? 97
Bodily privacy 98
Privacy of communications 99
Territorial privacy 100
A general cause of action for invasion of privacy? 102

6. The privacy principles

Introduction 106
Collection for lawful purposes – IPP 1; HPP 1 107
Collection directly from the individual – IPP 2; HPP 3 108
Further collection requirements – IPP 3 and IPP 4; HPP 4 111
Application of IPPs to records of observations or conversations 113
Retention and security of information – IPP 5; HPP 5 114
Access to, and alteration of, information – IPP 7 and IPP 8; HPP 8 115
The dichotomy between "use" and "disclosure" – IPPs 9, 10, 11 and 12; HPPs 9, 10, 11 and 12 117
Identification of the purpose for collection – IPPs 10 and 11; HPPs 10 and 11 119
Application of IPPS 10 and 11 and HPPs 10 and 11 to unsolicited information 120
Disclosure to third parties – IPP 11 122
Special restrictions on disclosure – IPP 12 123
Section 19(1) of PPIPA – disclosure of sensitive information 123
Section 19(2) of PPIPA – disclosure outside NSW 124
Regulating unique identifiers 126

7. Other operational issues

Introduction 130

Exemptions 131

Section 24 of PPIPA – exemptions relating to investigative agencies 131

Section 25 of PPIPA – exemptions where non-compliance is otherwise permitted 131

Application of s 25(b) to a preliminary inquiry by the Ombudsman 133

Privacy codes of practice - PPIPA Part 3; HRIPA Part 5 134

The meaning of “person” in s 37 and 38 of PPIPA.......................... 134

Public interest directions - PPIPA s 41 ; HRIPA s 62...................... 136

Complaints under s 45 of PPIPA.. 137

Complaints on behalf of the individual.. 137

Criteria to be applied by the Privacy Commissioner................... 137

Relationship between s 45 and s 36(2)(k) of PPIPA 138

Application of s 51 of PPIPA to withdrawn complaints 140

Report to Parliament under s 65 of PPIPA 140

Review of conduct by the ADT - PPIPA Part 5; HRIPA s 21 141

Nature of the jurisdiction... 141

Absence of a limitation period for review by the ADT................. 143

The ADT’s powers on review 145

Role of the Privacy Commissioner 146

Commissioner Determination model vs Tribunal Determination model 147

8. Relationship between PPIPA and other legislation

Introduction 150

The relationship between PPIPA and the *FOI Act* 151

Disclosure, access and correction provisions............................ 151

Complaints-handling and review provisions 155

Amalgamation of the oversight of privacy and FOI 156

The relationship between PPIPA and the LGA 160

The relationship between PPIPA and the SRA 163

Tables 167

Table of cases... 168

Table of legislation 170

Commonwealth 170

New South Wales.. 171

Northern Territory 172

Tasmania... 172

Victoria 172

Other 172

Bibliography 173

TERMS OF REFERENCE

In a letter to the Commission received on 11 April 2006, the Attorney General, the Hon R J Debus MP issued the following terms of reference:

Pursuant to section 10 of the *Law Reform Commission Act 1967* (NSW), the Law Reform Commission is to inquire into and report on whether existing legislation in New South Wales provides an effective framework for the protection of the privacy of an individual. In undertaking this review, the Commission is to consider in particular:

- The desirability of privacy protection principles being uniform across Australia.
- The desirability of a consistent legislative approach to privacy in the *Privacy and Personal Information Protection Act 1998*, the *Health Records and Information Privacy Act 2002*, the *State Records Act 1998*, the *Freedom of Information Act 1989* and the *Local Government Act 1993*.
- The desirability of introducing a statutory tort of privacy in New South Wales.
- Any related matters.

The Commission should liaise with the Australian Law Reform Commission which is reviewing the *Privacy Act 1988* (Cth) as well as other relevant Commonwealth, State and Territory agencies.

PARTICIPANTS

Division Members

Professor Michael Tilbury (Commissioner-in-charge)

The Hon James Wood AO QC

His Honour Judge Kevin O'Connor AM

Officers of the Commission

Executive Director	Mr Peter Hennessy
Legal research and writing	Ms Catherine Gray
	Ms Sharminie Niles
	Ms Donna Hayward
Paralegal assistance	Mr Michael Andrews
Librarian	Ms Anna Williams
Desktop publishing	Mr Terence Stewart
Administrative assistance	Ms Wendy Stokoe

SUBMISSIONS

The Commission invites submissions on the issues relevant to this review, including but not limited to the proposals and issues raised in this Consultation Paper.

All submissions and enquiries should be directed to:

Mr Peter Hennessy
Executive Director
NSW Law Reform Commission

Postal addresses: GPO Box 5199, Sydney NSW 2001
or DX 1227 Sydney

Street Address: Level 13, 10 Spring Street, Sydney NSW

Email: nsw_lrc@agd.nsw.gov.au

Contact numbers: Telephone (02) 8061 9270
Facsimile (02) 8061 9376

The closing date for submissions is 17 October 2008.

Confidentiality and use of submissions

In preparing further papers on this reference, the Commission will refer to submissions made in response to this Issues Paper. If you would like all or part of your submission to be treated as confidential, please indicate this in your submission. The Commission will respect requests for confidentiality when using submissions in later publications.

Copies of submissions made to the Commission will also normally be made available on request to other persons or organisations. Any request for a copy of a submission marked "confidential" will be determined in accordance with *the Freedom of Information Act 1989* (NSW).

Other publication formats

The Commission is committed to meeting fully its obligations under State and Commonwealth anti-discrimination legislation. These laws require all organisations to eliminate discriminatory practices which may prevent people with disabilities from having full and equal access to our services. This publication is available in alternative formats. If you have any difficulty in accessing this document please contact us.

LIST OF PROPOSALS AND ISSUES

PROPOSALS

Chapter 1

PROPOSAL 1 – *see page 4*

Reforms of New South Wales privacy law should aim to achieve national uniformity.

PROPOSAL 2 – *see page 4*

New South Wales should co-operate with the Commonwealth in the development of privacy principles that are capable of application in all New South Wales privacy legislation.

PROPOSAL 3 – *see page 4*

New South Wales legislation should only apply to the handling of personal information by public sector agencies.

Chapter 4

PROPOSAL 4 – *see page 58*

The *Privacy and Personal Information Protection Act 1998* (NSW) should be restructured:

- to locate the IPPs and exemptions in a schedule to the Act; and
- to reduce the Act's level of detail and complexity to resemble more closely that of the Health Records and Information Privacy Act 2002 (NSW).

PROPOSAL 5 – *see page 64*

The *Health Records and Information Privacy Act 2002* (NSW) should be amended so that the handling of health information by private sector organisations is regulated under the *Privacy Act 1988* (Cth).

Chapter 5

PROPOSAL 6 – *see page 95*

All State owned corporations should be covered by privacy legislation.

PROPOSAL 7 – *see page 96*

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that where a public sector agency contracts with a non-government organisation to provide services for government, the non-government organisation should be contractually obliged to abide by the IPPs and any applicable code of practice in the same way as if the public sector agency itself were providing the services.

Chapter 6

PROPOSAL 8 – *see page 110*

If the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) are merged, the provision governing collection of personal information directly from an individual should contain the two exceptions currently provided for in IPP 2 together with a third exception currently provided for in HPP 3, namely that information must be collected from the individual unless it is "unreasonable or impractical to do so".

PROPOSAL 9 – *see page 110*

If two separate Acts continue to operate:
HPP 3 should be amended to allow an individual to authorise collection of his or her personal information by an organisation from someone else and to allow collection of information about an individual under 16 years from a parent or guardian; and
IPP 2 should be amended by introducing a further exemption, namely, that information must be collected from the individual unless it is "unreasonable or impractical to do so".

PROPOSAL 10 – *see page 113*

IPPs 3 and 4 should be amended to stipulate that the requirements imposed by those sections apply whether the information is collected directly from the individual to whom the information relates or indirectly from someone else.

PROPOSAL 11 – *see page 114*

IPPs 3 and 4 should be amended to clarify that the word "collects" means, in relation to information derived from observations of, or conversations with, an individual, the point at which information is recorded.

PROPOSAL 12 – *see page 114*

IPP 5 and HPP 5 should be amended to include a requirement for the secure collection of personal information.

PROPOSAL 13 – *see page 116*

The meaning and effect of s 20(5) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 22(3) of the *Health Records and Information Privacy Act 2002* (NSW), and their application to the IPPs and HPPs respectively, should be clarified.

PROPOSAL 14 – *see page 126*

Section 19(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be redrafted in line with HPP 9 and the proposed UPP 11. Alternatively, if the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) are to become one Act, HPP 9, redrafted to incorporate elements of the proposed UPP 11, is to be preferred over s 19(2) to regulate transborder data flows and transfer of information to Commonwealth agencies.

PROPOSAL 15 – *see page 128*

If the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) are to become one Act, a privacy principle regulating the use and disclosure of identifiers should be contained in the new Act. If the two Acts are to remain separate, the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended by the addition of a further IPP regulating the use and disclosure of identifiers.

Chapter 7

PROPOSAL 16 – *see page 133*

Section 25(b) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to read as follows:
"A public sector agency is not required to comply with section 9, 10, 13, 14, 15, 17, 18 or 19 if:
…
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act (including the *State Records Act 1998*) or any other law."

PROPOSAL 17 – *see page 136*

Section 41 of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 62 of the *Health Records and Information Privacy Act 2002* (NSW) should be amended to give the Privacy Commissioner the power to amend an earlier direction.

PROPOSAL 18 – *see page 145*

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a limitation period for application for review by the Administrative Decisions Tribunal of an internal review. This should provide that an application to the Administrative Decisions Tribunal for external review of a complaint must be made within 60 days after the applicant:
(a) is notified that the Privacy Commissioner refuses to investigate the conduct complained of; or
(b) receives a report of the results of the Privacy Commissioner's investigation.

PROPOSAL 19 – *see page 146*

Section 55(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that the Administrative Decisions Tribunal may make any one or more of the orders listed in subsections (a)-(g) on finding that the public sector agency's conduct the subject of the review was conduct that:

- contravened an IPP that applied to the agency;
- contravened a privacy code of practice that applied to the agency; or
- amounted to disclosure by the agency of private information kept in a public register.

PROPOSAL 20 – *see page 147*

Section 56 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a provision that the Privacy Commissioner has a right to appear and be heard in any proceedings before the Appeal Panel of the Administrative Decisions Tribunal.

ISSUES

Chapter 1

ISSUE 1 – *see page 7*

(a) What are the impediments to information sharing in New South Wales?

(b) How should they be resolved?

ISSUE 2 – *see page 8*

To what extent are the criminal sanction provisions of the legislation considered in this paper adequate and satisfactory?

Chapter 4

ISSUE 3 – *see page 60*

Should the *Privacy and Personal Information Protection Act 1998* (NSW) contain an objects clause? If so, how should that clause be drafted?

ISSUE 4 – *see page 66*

If health information held by the private sector were to be regulated by the *Privacy Act 1988* (Cth), should New South Wales continue to have two separate information privacy statutes?

ISSUE 5 – *see page 66*

What reasons would there be for the continued existence of the *Health Records and Information Privacy Act 2002* (NSW) if it only regulated public sector agencies?

Chapter 5

ISSUE 6 – *see page 82*

(a) Should "publicly available information" under the *Privacy and Personal Information Protection Act 1998* (NSW) and "generally available information" under the *Health Records and Information Privacy Act 2002* (NSW) be exempted altogether from the definition of "personal information" in those Acts?

(b) Should IPP 2 and HPP 2 alone apply to "publicly available information" and "generally available information", but not other IPPs and HPPs?

ISSUE 7 – *see page 82*

(a) Is the meaning of "publicly available information" the same as "generally available information"? Is it appropriate that they have different meanings in the context of general information and health information?

(b) If two different phrases are to remain, should the definitions of "publicly available information" and "generally available information" be clarified in the legislation?

ISSUE 8 – *see page 82*

(a) Should the exemptions in any or all of the following provisions remain or are they made unnecessary by s 20(5) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 22(3) of the *Health Records and Information Privacy Act 2002* (NSW) and Schedule 1 to the *Freedom of Information Act 1989* (NSW):

- **s 4(3)(e) of the Privacy and Personal Information Protection Act 1998 (NSW) and s 5(3)(h) of the Health Records and Information Privacy Act 2002 (NSW);**
- **s 4(3)(i) of the Privacy and Personal Information Protection Act 1998 (NSW) and s 5(3)(l) of the Health Records and Information Privacy Act 2002 (NSW); and/or**

- **s 4(3)(ja) of the Privacy and Personal Information Protection Act 1998 (NSW)?**

(b) If any or all of the exemptions are to remain, should the information referred to in each provision be exempt from all the IPPs and HPPs or only some of them? Which, if any, IPPs and HPPs should apply to the information?

(c) If the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) are merged into one Act, how should the exemptions be worded if they are retained?

ISSUE 9 – *see page 83*

What is the rationale behind, and value of, the exception contained in s 4(3)(h) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(3)(k) of the *Health Records and Information Privacy Act 2002* (NSW) (information arising out of a complaint about conduct of police officers)?

ISSUE 10 – *see page 83*

Should a person who has made a complaint about police conduct be precluded from having access to their personal file in relation to the complaint process?

ISSUE 11 – *see page 83*

Should the police officer who is the subject of a complaint be able to access the information relating to the complaint?

ISSUE 12 – *see page 83*

Should some IPPs and HPPs but not others apply to information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990* (NSW)? If so, which ones should apply?

ISSUE 13 – *see page 83*

(a) Should the NSW Ombudsman be included among those agencies listed in s 27 of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 17 of the *Health Records and Information Privacy Act 2002* (NSW) as being exempt from compliance with the IPPs?

(b) Even if the answer to this is "yes", should the information referred to in s 4(3)(c), (d), (f) and (h) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(3)(f), (g), (i) and (k) of the *Health Records and*

***Information Privacy Act 2002* (NSW) continue to be exempt from the definition of "personal information"?**

ISSUE 14 – *see page 83*

Should the legislation continue to exempt from the definition of "personal information" information about an individual's suitability for appointment or employment as a public sector official?

ISSUE 15 – *see page 84*

Should the exemption from the definition of "personal information" of information about an individual's suitability for appointment or employment as a public sector official be restricted to information about a prospective employee, or also apply to information about an agency's current employee?

ISSUE 16 – *see page 84*

Do s 4(3)(j) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(3)(m) of the *Health Records and Information Privacy Act 2002* (NSW) need amending to clarify their meaning and Parliament's intention?

ISSUE 17 – *see page 84*

Should s 4(3)(j) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(3)(m) of the *Health Records and Information Privacy Act 2002* (NSW) be reworded to provide that they apply only to information that directly relates to suitability for recruitment, promotion, discipline and involuntary retirement?

ISSUE 18 – *see page 84*

(a) Should information contained in photographs or video images come within the definition of "personal information"?

(b) Should this depend on whether an individual's identity is apparent or can reasonably be identified from the visual image?

(c) If the definition of "personal information" should include visual images, should this be clarified in the legislation?

(d) Should some of the IPPs, but not others, apply to visual images that contain personal information? If so, which ones should apply?

ISSUE 19 – *see page 84*

(a) Should the meaning of the phrase "or can reasonably be ascertained from the information or opinion" in s 4(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(1) of the *Health Records and Information Privacy Act 2002* (NSW) be clarified?

(b) If so, should this be by an amendment to the legislation or should it be left to judicial construction or the publication of a Privacy Guideline?

ISSUE 20 – *see page 86*

Should s 3(1)(b) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to define a "public sector agency" as "a body established or appointed for a public purpose by or under a NSW Act " or, alternatively, "any public authority constituted by or under a NSW Act"?

ISSUE 21 – *see page 86*

Should s 4(1) of the *Health Records and Information Privacy Act 2002* (NSW) be amended to define a "public sector agency" as "a body established or appointed for a public purpose by or under a NSW Act or an affiliated health organisation" or, alternatively, "any public authority constituted by or under a NSW Act or an affiliated health organisation"?

ISSUE 22 – *see page 89*

Should the meaning of "unsolicited" in s 4(5) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 10 of the *Health Records and Information Privacy Act 2002* (NSW) be clarified?

ISSUE 23 – *see page 89*

If information is "unsolicited", what IPPs or HPPs, if any, should apply to that information? Should all of the provisions of the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) apply to unsolicited information, except the collection IPPs and HPPs?

ISSUE 24 – *see page 92*

Should the meaning of, and distinction between, "administrative" and "educative" functions in s 27 of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 17 of the *Health Records and Information Privacy Act 2002* (NSW) be more clearly defined?

ISSUE 25 – *see page 92*

Should the legislation explicitly provide that if a function is dual, the administrative function must be separately categorised?

ISSUE 26 – *see page 92*

Is the opportunity to complain to the Privacy Commissioner and challenge the categorisation of a function sufficient?

ISSUE 27 – *see page 99*

Should the *Privacy and Personal Information Protection Act 1998* (NSW) contain express provisions for the general regulation of bodily privacy?

ISSUE 28 – *see page 101*

Should the *Privacy and Personal Information Protection Act 1998* (NSW) contain express provision for breaches of territorial privacy?

ISSUE 29 – *see page 103*

If a statutory cause of action for invasion of privacy is to be enacted, what should be its relationship to the *Privacy and Personal Information Protection Act 1998* (NSW)?

Chapter 6

ISSUE 30 – *see page 108*

Should IPP 1 be amended to include a provision that a public sector agency must not collect personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, sexual activities or criminal record (defined as "sensitive information") unless the collection is strictly necessary?

ISSUE 31 – *see page 108*

Should collection of sensitive information be allowed if necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person?

ISSUE 32 – *see page 110*

Should the *Privacy and Personal Information Protection Act 1998* (NSW) be amended by introducing a provision equivalent to s 7 of the *Health Records and Information Privacy Act 2002* (NSW) that an individual is incapable of doing an act authorised, permitted or required by the *Health Records and Information Privacy Act 2002* (NSW) if that individual is

incapable, by reason of age, injury, illness or physical or mental impairment, of understanding the nature of the act or communicating his or her intentions with respect to the act?

ISSUE 33 – *see page 113*

Should IPP 3 be amended to adopt the wording of HPP 4 or UPP 3.2, or some combination of the two?

ISSUE 34 – *see page 114*

Should IPP 9 and HPP 9 apply to personal information that consists of conclusions drawn, or opinions expressed, based on observations of, or conversations with, an individual, providing a record is made of those conclusions or opinions? If so, do these provisions require amendment to clarify this?

ISSUE 35 – *see page 117*

Does the effect of s 15(1) and (2) of the *Privacy and Personal Information Protection Act 1998* (NSW) need clarification? If so, how should one or both sections be amended to reconcile their operation?

ISSUE 36 – *see page 119*

(a) Should "use" and "disclosure" be treated as one concept such as "processing", or as a combined phrase such as in the proposed UPP 5, with the one set of privacy standards and exemptions applying?

(b) Alternatively, should the same privacy standards, and exemptions from those standards, contained in the HPPs apply equally to "use" and "disclosure" of information?

ISSUE 37 – *see page 120*

Is the correct interpretation of IPPs 10 and 11 and HPPs 10 and 11 that the relevant purpose is the one for which the agency/organisation collected it? If so, should the provisions be amended to clarify this?

ISSUE 38 – *see page 121*

Do IPPs 10 and 11 and HPPs 10 and 11 apply to unsolicited information? If not, should they apply?

ISSUE 39 – *see page 121*

Should the privacy principles include a principle in terms identical, or equivalent, to the proposed UPP 2.5?

ISSUE 40 – *see page 122*

(a) Should s 18(1)(b) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to include the phrase "and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure"?

(b) Alternatively, should s 18(1)(b) be amended to delete the reference to s 10 and to provide instead that the individual must be made aware at the time the information is collected that information of that kind is usually disclosed to a third party?

ISSUE 41 – *see page 124*

Should disclosure of an individual's criminal history and record be restricted under s 19 of the *Privacy and Personal Information Protection Act 1998* (NSW)?

ISSUE 42 – *see page 124*

Should the meaning of the words "sexual activities" in s 19(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) be clarified?

ISSUE 43 – *see page 124*

Should s 19(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) be taken out of s 19 and placed within s 18?

ISSUE 44 – *see page 128*

Should the privacy principle regulating the use and disclosure of identifiers be in the same terms as HPP 12 or the proposed UPP 10, or some combination of the two?

Chapter 7

ISSUE 45 – *see page 131*

Should s 24 of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to exempt an agency from compliance with IPPs 2, 3, 10 and 11 when the agency is disclosing personal information to an investigative agency for the purpose of that investigative agency carrying out its complaint handling or investigative functions?

ISSUE 46 – *see page 132*

(a) Is the correct interpretation of s 25(a) of the *Privacy and Personal Information Protection Act 1998* (NSW) that it applies to cases where a statutory provision expressly refers to the relevant IPP and provides that an agency is authorised or required not to comply with it, or is a wider interpretation correct, such as adopted by the Administrative Decisions Tribunal in *HW v Commissioner of Police, New South Wales Police Service*?

(b) Should s 25(a) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to clarify its application?

ISSUE 47 – *see page 134*

Should public sector agencies be exempted from compliance with s 18 of the *Privacy and Personal Information Protection Act 1998* (NSW) if the information is disclosed to an investigative agency in order that it may exercise its complaints-handling or investigative functions?

ISSUE 48 – *see page 134*

Should the interaction of s 29(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) with s 30(1) of that Act be clarified?

ISSUE 49 – *see page 134*

Should the precise scope of a privacy code of practice be clarified?

ISSUE 50 – *see page 135*

Should the word "person" in s 37 and 38 of the *Privacy and Personal Information Protection Act 1998* (NSW) be read as meaning a "natural person"? If so, should this be clarified in the legislation?

ISSUE 51 – *see page 135*

Should both s 37 and 38(4) of the *Privacy and Personal Information Protection Act 1998* (NSW) apply to a "person or public sector agency"?

ISSUE 52 – *see page 137*

(a) Should the intended application of s 41 of the Privacy and Personal Information Protection Act 1998 (NSW) and s 62 of the Health Records and Information Privacy Act 2002 (NSW) be clarified?

(b) Should the sections make clear that the Privacy Commissioner may make a written direction applying to a class of agency/organisation?

(c) Alternatively, should the sections make clear that the Privacy Commissioner may not make a written direction applying to a class of agency/organisation?

ISSUE 53 – *see page 137*

Should s 45(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to clarify that its application is limited to an individual whose privacy has been violated, or a person acting on behalf of the individual?

ISSUE 54 – *see page 138*

Should the meaning of "violation of" and "interference with" an individual's privacy in s 45(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) be clarified?

ISSUE 55 – *see page 138*

Should the legislation provide guidelines as to what can be taken into account in determining whether there has been a "violation of, or interference with, the privacy of an individual"?

ISSUE 56 – *see page 139*

(a) Does the interaction between, and operation of, s 45 and 36(2)(k) of the *Privacy and Personal Information Protection Act 1998* (NSW) need to be clarified?

(b) Should these sections be regarded as together regulating the Privacy Commissioner's functions and powers with respect to complaints or as two independent sources of the Privacy Commissioner's powers?

ISSUE 57 – *see page 139*

Does s 51 of the *Privacy and Personal Information Protection Act 1998* (NSW) require clarification with respect to the Privacy Commissioner's power to conduct an inquiry or investigation into any general issue raised by a withdrawn complaint?

ISSUE 58 – *see page 141*

(a) Is it correct to conclude that the Privacy Commissioner has the power to make a "special report" under s 65 of the *Privacy and Personal Information Protection Act 1998* (NSW) in relation to a complaint made under s 45, in addition to the power to make a report under s 50 of that Act?

(b) Should the legislation be amended to clarify the Privacy Commissioner's powers under s 65 and s 50 of the *Privacy and Personal Information Protection Act 1998* (NSW) to make a report relating to a complaint made under s 45?

ISSUE 59 – *see page 143*

(a) Should s 55 of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to clarify whether an application to the Administrative Decisions Tribunal is heard in its original or review jurisdiction?

(b) Should the jurisdiction be specified as being "review"?

ISSUE 60 – *see page 145*

Should s 53(3) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to include a provision allowing a person to request internal review of conduct outside the six-month limitation period?

ISSUE 61 – *see page 148*

Should Part 5 of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to give final determination of a complaint to the Privacy Commissioner rather than the Administrative Decisions Tribunal?

Chapter 8

ISSUE 62 – *see page 154*

Should the disclosure, access and correction provisions of the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Freedom of Information Act 1989* (NSW) be rationalised?

ISSUE 63 – *see page 154*

Should the Freedom of Information Act 1989 (NSW) be the means by which the *Privacy and Personal Information Protection Act 1998* (NSW) access rights are obtained?

ISSUE 64 – *see page 156*

Should the complaints-handling and review procedures of the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Freedom of Information Act 1989* (NSW) that are not specifically related to the particular provisions of each Act be made consistent?

ISSUE 65 – *see page 159*

Should the administration of FOI and privacy legislation be amalgamated in one body?

ISSUE 66 – *see page 163*

(a) Should the following amendments, as suggested by the NSW Ombudsman, be made?

- **repeal s 20(5) of the *Privacy and Personal Information Protection Act 1998* (NSW);**
- **amend s 13, 14 and 15 and/or s 20 of the *Privacy and Personal Information Protection Act 1998* (NSW) to provide that the IPPs contained in those sections do not apply to agencies to which the *Freedom of Information Act 1989* (NSW) applies and that, in relation to those agencies, those principles are implemented through the relevant provisions of the *Freedom of Information Act 1989* (NSW);**
- **amend the *Freedom of Information Act 1989* (NSW) to clarify that agencies can adopt informal methods of releasing personal information to the applicant.**

(b) Is there a better alternative to this solution?

ISSUE 67 – *see page 163*

What alternative amendments to the *Privacy and Personal Information Protection Act 1998* (NSW), the *Freedom of Information Act 1989* (NSW) and the *Local Government Act 1993* (NSW) would address the current problems arising from the application of three different regulatory schemes?

ISSUE 68 – *see page 165*

(a) Should a provision be inserted into s 12 of the *Privacy and Personal Information Protection Act 1998* (NSW), identical to that inserted into s 15(4) of that Act, providing that s 12, and any provision of a privacy code of practice that relates to the requirements set out in that section, apply to public sector agencies despite s 21 of the *State Records Act 1998* (NSW)?

(b) Alternatively, should s 12 be clarified as taking effect subject to the prohibition in s 21 of the *State Records Act 1998* (NSW)?

1. Introduction

- Putting this paper in context
- Further issues
- An outline of the chapters

PUTTING THIS PAPER IN CONTEXT

1.1 In May 2007, the Commission published a consultation paper on the desirability of introducing a statutory cause of action for breach of privacy in New South Wales.[1] This was the broadest, and possibly the most difficult, issue we were required to consider in reviewing generally whether existing legislation in New South Wales is effective in protecting individual privacy.[2]

1.2 Other specific issues the Commission was asked to inquire into were:

- the advantages of uniform privacy protection principles across Australia; and
- the desirability of a consistent legislative approach to privacy within NSW itself.

1.3 This consultation paper focuses on the second issue and evaluates the effectiveness of the key New South Wales statutes that protect privacy. These are: the *Privacy and Personal Information Protection Act 1998* (NSW) ("PPIPA"); the *Health Records and Information Privacy Act 2002* (NSW) ("HRIPA"); the *Freedom of Information Act 1989* (NSW); the *Local Government Act 1993* (NSW); and the *State Records Act 1998* (NSW).

1.4 The first issue, uniform privacy protection, is one of the key areas of focus of a concurrent inquiry into privacy laws by the Australian Law Reform Commission ("ALRC").[3] Our terms of reference specifically require us to liaise with the ALRC in conducting our review.

ALRC'S review of privacy law

1.5 In September 2007, the ALRC published a comprehensive discussion paper on Australia's privacy laws, containing a review of the *Privacy Act 1988* (Cth) ("*Privacy Act*") and related Commonwealth legislation, State and Territory regulation of privacy, and legislative and non-legislative rules, codes and guidelines. It contains approximately 300 proposals for reform. While its focus is on regulation at the federal level, there is nonetheless substantial overlap between the inquiries. For example, the impact of technology on

---

1. New South Wales Law Reform Commission, *Invasion of Privacy* (Consultation Paper 1, 2007).
2. Terms of Reference are set out at p viii.
3. See Australian Law Reform Commission, *Review of Privacy* (Issues Paper 31, 2006); Australian Law Reform Commission, *Review of Privacy* (Discussion Paper 72, 2007).

privacy, including surveillance, the internet, smart cards and DNA-based technologies, is relevant at all levels. The Commission will not duplicate research and consultation in areas of common concern and relevance. For this reason, this consultation paper is confined to State-specific privacy laws, namely the ones noted in paragraph 1.3 above.

1.6 The cornerstone of the ALRC report is the premise that privacy laws should be consistent across all Australian jurisdictions.[4] To that end, the ALRC proposes the development of Unified Privacy Principles ("UPPs") and the enactment by the States and Territories of legislation that applies these and adopts relevant definitions used in the *Privacy Act*.[5] The Commission fully supports this proposal for the reasons set out below, and this consultation paper should be considered in that context.

1.7 The ALRC noted that all the submissions it received in response to its Issues Paper 31, *Review of Privacy*, that addressed the issue of national consistency strongly endorsed its importance.[6] A nationally consistent privacy regime would: "lessen unjustified compliance burden and cost",[7] especially for those organisations and agencies that operate across State borders; lessen confusion about who to approach to make a privacy complaint; and remove impediments to information sharing and national initiatives.[8] This need for national consistency is heightened in an increasingly technology-driven world, where information is received and shared via the internet and other electronic devices and pathways.

1.8 We endorse the ALRC's conclusion that:

> A nationally consistent privacy regime will ensure that Australians' personal information will attract similar protection whether that personal information is being handled by an Australian Government agency or a state or territory government agency, a multinational organisation or a small business, and whether that information is recorded in a paper file or electronically.[9]

1.9 The Commission also notes that the Commonwealth Senate Committee privacy inquiry and the Commonwealth Office of the Privacy Commissioner Review both concluded that privacy laws should be consistent across Australia.[10] Further, the pursuit of

---

4. ALRC DP 72, [1.5].
5. ALRC DP 72, Proposal 4-4.
6. ALRC DP 72, [4.11].
7. ALRC DP 72, [4.11].
8. ALRC DP 72, [4.14].
9. ALRC DP 72, [4.16].
10. Senate Legal and Constitutional References Committee, Parliament of Australia, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005),

uniform law initiatives has been our goal in all appropriate areas of law reform in NSW. For example, in Report 107, *Guaranteeing Someone Else's Debts*, we recommended that the reform of the law of New South Wales relating to contracts guaranteeing another's debt would only make sense in the context of a uniform law reform initiative.[11]

PROPOSAL 1

Reforms of New South Wales privacy law should aim to achieve national uniformity.

1.10 The ALRC proposes that there be some flexibility in the application of the UPPs and that they be drafted at a high level of generality.[12] The Commission agrees that this is the right approach in order to accommodate the differences in practices and obligations across jurisdictions, public and private sectors, and individual businesses. It would also mean that uniform principles could be adopted across New South Wales privacy legislation, eliminating the need for separate Health Privacy Principles.

PROPOSAL 2

New South Wales should co-operate with the Commonwealth in the development of privacy principles that are capable of application in all New South Wales privacy legislation.

1.11 The ALRC also proposes that the *Privacy Act* should apply to all private sector organisations - State, Territory and Commonwealth - so that the States only regulate handling of personal information by its public sector agencies.[13] This would result in the exemption from HRIPA of private sector health agencies. The Commission favours this approach and discusses this option in Chapter 3.

PROPOSAL 3

New South Wales legislation should only apply to the handling of personal information by public sector agencies.

The purpose of this paper

1.12 This paper examines in detail the adequacy of the provisions of PPIPA and HRIPA and related Acts, considering how they could be

---

Rec 3; Office of the Privacy Commissioner, *Getting in on the Act: The Review of Private Sector Provisions of the Privacy Act 1988* (2005), Recs 2-7.

11. New South Wales Law Reform Commission, *Guaranteeing Someone Else's Debts* (Report 107, 2006), Rec 4.1.
12. See ALRC DP 72, vol 2 pt D.
13. ALRC DP 72, Proposal 4-1.

amended to operate more effectively. On one view, this could be seen as a redundant exercise if there is to be a national overhaul of privacy laws that remakes existing frameworks and principles. Furthermore, the current legislation may not be the best platform for reform in meeting the challenges posed by existing and emerging technologies.

1.13 The attainment of national uniformity cannot, however, be assumed. Even if uniformity is eventually achieved, the process of developing UPPs and achieving consistency between the federal and State and Territory jurisdictions may be a lengthy one. This phase of our inquiry points to the need for reform in detail of PPIPA and HRIPA in order to enable public sector agencies in particular to achieve the more certain, efficient and fairer protection of the privacy of individuals. In doing so, our inquiry informs the debate about the development of any proposed new national regulatory framework. In short, it represents a step along the continuum of privacy reform.

1.14 Moreover, as has been pointed out above, uniformity is not necessarily pursued or achieved in detail: it may be more about uniformity at the level of principle. Uniform principles are applied in New South Wales legislation in a way that is relevant to this jurisdiction. The proposed UPPs, for example, are stated at such a high level of generality that implementation will necessarily depend on mechanisms and processes at State level. The enforcement mechanisms adopted in New South Wales legislation and the role of the Privacy Commissioner in New South Wales are necessarily questions that must be addressed from a New South Wales perspective, even if they are to operate within a national framework.

FURTHER ISSUES

1.15 The paper focuses on the detail of legislation as it currently operates in NSW. However, we are conscious that our terms of reference require us generally to inquire into "whether existing legislation in New South Wales provides an effective framework for the protection of the privacy of an individual".[14] There are two factors in particular that are relevant to an effective framework that the Commission intends to investigate further. These are:

- the extent to which appropriate information sharing is actually occurring in New South Wales; and
- the extent to which the criminal provisions of New South Wales privacy legislation are working appropriately.

14. Terns of reference are at p viii.

Information sharing

1.16 We agree with the ALRC that "appropriate" information sharing, compliant with privacy laws, should be encouraged.[15] Yet, as the ALRC has documented, a "risk averse" interpretation of privacy laws, encouraged by the difficulties of complying with inconsistent, fragmented and multi-layered privacy legislation, can result in a reluctance by agencies and organisations to share information.[16] While this can impact on business as a compliance cost,[17] its most serious impact is in the provision of services to vulnerable people, particularly in the area of child protection,[18] which we take as an example.

1.17 It is obviously essential to have a simple and practical system for the exchange of information between agencies that promotes the safety, welfare and well-being of children. Section 248 of the *Children and Young Persons (Care and Protection) Act 1998* (NSW) provides that the Department of Community Services ("DOCS") may exchange information about a child with a prescribed body, but not that these prescribed bodies may exchange information with each other. Prescribed bodies include the Police Service, government departments, schools, TAFEs, hospitals, fostering agencies, child care centres, adoption agencies, the Family Court of Australia and Centrelink, among others.

1.18 As the law currently stands, agencies or organisations sharing information with each other may be in breach of s 248 of the *Children and Young Persons (Care and Protection) Act 1998* (NSW) or of PPIPA, HRIPA or the *Privacy Act*, or may even be committing an offence under s 254 of the *Children and Young Persons (Care and Protection) Act 1998* (NSW). That section provides that it is an offence for a person to disclose any information obtained in connection with the administration or execution of the Act. Yet not to share information either forces the agency or organisation to go through DOCS, when this may not be appropriate or otherwise necessary, or hinders the crucial role that these bodies play in protecting and caring for children. Limiting the scope of s 248 fails to recognise the common scenario where various agencies and organisations have different responsibilities in relation to a particular child and need to share information with each other to provide joint support for the child.[19]

---

15. ALRC DP 72, [11.10]-[11.11].
16. ALRC DP 72, [11.1]-[11.9].
17. ALRC DP 72, [11.9].
18. See ALRC DP 72, [11.8].
19. Examples include: carrying out a risk assessment of a child; principals of schools notifying each other of a "risk of harm" situation where the child has changed schools; or an agency obtaining police information to investigate

1.19 Some options to address this problem are to expand s 248 to allow inter-agency information sharing, or to formulate Privacy Codes of Practice under PPIPA and HRIPA. The definition of "human services" in the Health Records And Information Privacy Code of Practice 2005 and in Part 4 of the Privacy Code of Practice (General) 2003, which allow public and private organisations that provide "human services" to collect, use and disclose personal information about an individual to each other, could be expanded by explicitly including agencies that provide children's or policing services. Alternatively PPIPA and HRIPA could be amended to deal specifically with the problem and the impact of s 248.

1.20 The Commission invites submissions on the extent to which there are cultural and legal impediments to appropriate information sharing in New South Wales. We also invite submissions on how the issue should be addressed.

ISSUE 1

(a) What are the impediments to information sharing in New South Wales?

(b) How should they be resolved?

Criminal sanctions

1.21 In our consultation paper, *Invasion of Privacy*, we outlined the extent to which the criminal law protects individuals against privacy invasions.[20] Section 62 and s 63 of PPIPA impose criminal sanctions for, respectively: corrupt disclosure and use of personal information by a public sector official; and offering to supply personal information that has been disclosed unlawfully. Section 67 imposes criminal sanctions on the Privacy Commissioner or a staff member for disclosure of information otherwise than in accordance with the legislation. Section 68 imposes criminal sanctions in relation to dealings with the Privacy Commissioner.

1.22 In line with s 62 and 63 of PPIPA, s 68 and 69 of HRIPA impose criminal sanctions for, respectively: corrupt disclosure and use of health information by a public sector official; and offering to supply health information that has been disclosed unlawfully. Section 70 of HRIPA imposes criminal sanctions for using threats, intimidation or misrepresentations to: (1) stop, or try to stop, a person from requesting access to health information, making a complaint to the Privacy

---

allegations against an employee, particularly where that employee is working with children.

20. New South Wales Law Reform Commission, *Invasion of Privacy* (Consultation Paper 1, 2007), [2.90]-[2.112].

Commissioner or Tribunal, or applying for review of conduct, or from withdrawing a request, complaint or application; or (2) force a person to give consent or to do something without consent, where the Act requires consent.

1.23 While the Commission is aware of one pending case under privacy laws,[21] the criminal sanction provisions of the legislation considered in this consultation paper do not appear to have been used in practice. We invite submissions on the extent to which the provisions are adequate and satisfactory with a view to determining the extent to which they ought to be used as a method of protecting individual privacy.

ISSUE 2

To what extent are the criminal sanction provisions of the legislation considered in this paper adequate and satisfactory?

AN OUTLINE OF THE CHAPTERS

1.24 The substantive part of the paper begins, in Chapters 2 and 3, with an overview of the current federal and New South Wales privacy statutes. Chapter 2 focuses on federal privacy laws, in particular, the *Privacy Act*. Chapter 3 describes the operation and provisions of PPIPA and HRIPA and provides a summary of the Information Protection Principles and Health Privacy Principles, their roles and purposes, applicable exemptions and complaints-handling mechanisms.

1.25 Chapter 4 examines ways of achieving greater consistency of structure within and between New South Wales privacy laws. In particular, the chapter seeks views on:

- whether the structural basis of PPIPA and HRIPA is the most effective way of promoting the aims of each piece of legislation;
- whether New South Wales should continue, under HRIPA, to regulate the privacy of health information handled by the private sector, given the ALRC's proposal for this to be regulated nationally; and
- whether, in the light of the above point, if HRIPA is restricted to the regulation of health information held by the public sector

21. In a case not heard at the time of writing, two police officers were charged with unlawfully disclosing personal information after they disclosed to a man in their custody that his girlfriend was born a male but underwent gender reassignment surgery: Kim Arlington, "Accused joked about transvestite lover he allegedly assaulted" *The Daily Telegraph* (Sydney), 6 February 2008.

only, the need for separate health privacy legislation in New South Wales persists.

1.26 Chapter 5 inquires into whether the scope of PPIPA and/or HRIPA can or should be extended: by limiting the numerous exemptions in the legislation, particularly exemptions to the definition of "personal information"; and/or by giving express protection to areas, subject matters or activities beyond information privacy. It also considers whether an expanded range of remedies should be made available under PPIPA for breaches of privacy. The chapter then discusses the prospect of a statutory cause of action for invasion of privacy and how this would intersect with PPIPA and HRIPA and other privacy laws.

1.27 Chapters 6 and 7 take the inquiry to a more detailed level. They identify specific problems with the operation of particular provisions of PPIPA and HRIPA. Chapter 6 focuses on the difficulties that agencies and the public experience in relation to the operation of the Privacy Principles. Chapter 7 examines issues relating to: s 37 and 38 of PPIPA; privacy codes of practice; public interest directions; complaints about, and review of, agency/organisation conduct; and two exemptions arising from s 24 and 25 of PPIPA.

1.28 As well as the ALRC's review of privacy laws, the NSW Health Department is presently conducting a statutory review of HRIPA. The Commission will draw on the findings of both those reviews in formulating our final recommendations. The chapters do, however, raise 68 issues for community consultation and response and make 20 proposals for reform.

1.29 Chapter 8 examines the relationship of PPIPA to other statutes that afford privacy protection, namely the *Freedom of Information Act 1989* (NSW), the *Local Government Act 1993* (NSW) and the *State Records Act 1998* (NSW). It examines the duplication and inconsistencies between PPIPA and these statutes. It also considers the arguments for and against amalgamation of the oversight of privacy and freedom of information.

2. Current privacy protection - Commonwealth

- Introduction
- The Privacy Act 1988 (Cth)
- Other federal privacy legislation

INTRODUCTION

2.1 The law of privacy in New South Wales is regulated by federal and State privacy legislation, primarily in relation to information privacy. These statutes govern the conduct of government agencies and in some cases, the private sector, when dealing with the subject matter of the relevant legislation. While they do impose penalties, they do not generally provide for civil liability for breach of their provisions.

2.2 The common law of Australia protects privacy interests in specific causes of action but does not provide a general civil cause of action. However, as discussed in more detail in Chapter 5, the Commission has recently published a Consultation Paper that considers the need for such a cause of action.[1]

2.3 This chapter provides an overview of the current federal privacy statutes, focusing on the *Privacy Act 1988* (Cth). It summarises the Act's coverage, the role and purpose of the information privacy principles, the applicable exemptions and the complaints handling mechanisms. The following chapter engages in a similar exercise in relation to privacy laws operating in New South Wales, primarily the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW).

THE PRIVACY ACT 1988 (CTH)

2.4 The *Privacy Act 1988* (Cth) ("*Privacy Act*") is the key piece of federal privacy legislation regulating the handling of an individual's personal information. It applies to both the public and private sectors in relation to the acts done and practices engaged in by agencies or organisations, subject to a wide range of exceptions and exemptions.

2.5 When first enacted in 1988, the *Privacy Act* regulated the collection, storage, use and disclosure of "personal information" by Australian Government departments and agencies only, by means of a set of 11 Information Privacy Principles ("Commonwealth IPPs"). "Personal information" was, and is, defined as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."[2]

1. New South Wales Law Reform Commission, *Invasion of Privacy* (Consultation Paper 1, 2007).
2. *Privacy Act 1988* (Cth) s 6(1).

2.6 Since its passage in 1988, the *Privacy Act* has been amended on several occasions. Notably, in 1994, when the ACT public service was established as a separate entity from the Australian Government, amendments were made to continue coverage for ACT public service agencies.[3] In 1990, coverage was extended to provide safeguards for individuals in relation to consumer credit reporting.[4] In 2000, coverage was further extended to include private sector entities and a further set of privacy principles, known as the National Privacy Principles ("NPPs"), was incorporated into the *Privacy Act*. The types of entities covered are included within the definition of an "organisation". These are: an individual, body corporate, partnership, or any other unincorporated association or trust.[5]

2.7 Thus, the *Privacy Act* now regulates the Australian Government and ACT public sector through its 11 Commonwealth IPPs, and the private sector through its 10 NPPs subject to a wide range of specified exceptions and exemptions.

2.8 Although it has wide coverage within the area of information privacy, the *Privacy Act* is not intended to cover the field.[6] It does not regulate the handling of personal information by the New South Wales public service, which is regulated by the *Privacy and Personal Information Protection Act 1988* (NSW). It does, however, apply to the private sector including private sector health service providers. The latter are also covered under the *Health Records and Information Privacy Act 2002* (NSW), creating some overlap.[7]

The Commonwealth Information Privacy Principles

2.9 The Commonwealth IPPs, set out in s 14 of the *Privacy Act*, regulate the way in which Australian Government agencies should handle personal information. The individuals and bodies to whom the principles apply are: ministers, departments, federal courts, the Australian Federal Police and other bodies or tribunals established or appointed for a public purpose.[8] In summary, the Commonwealth IPPs set the following parameters:

---

3. *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth).
4. *Privacy Act 1988* (Cth) pt IIIA.
5. *Privacy Act 1988* (Cth) s 6C(1).
6. See Australian Law Reform Commission, *Review of Privacy* (Discussion Paper 72, 2007).
7. This is discussed further in Chapter 3.
8. *Privacy Act 1988* (Cth) s 6(1).

- Personal information should only be collected for a lawful purpose that is necessary for, or directly related to, the function of the agency and must not be collected by unlawful or unfair means.[9]
- When soliciting information from an individual, the individual must be made aware of the purpose for which the information is collected, whether the collection of the information is authorised or required by law, and the agency's usual practices regarding disclosure.[10]
- When soliciting information generally, the information collected must be relevant, up to date and complete. The collection of the information must not intrude unreasonably upon the personal affairs of the individual.[11]
- Storage and security of personal information is regulated[12] and an agency is required to keep records of the type of information that is held.[13]
- Agencies are also required to give persons access to their personal information unless such access is excepted by law.[14] They are also required to make any necessary amendments to ensure that the information is accurate and up-to-date.[15] Such information must be accurate[16] and should only be used for a purpose to which the information is relevant.[17]
- Where the information is obtained for a particular purpose, there are limits on the use of such information for any other purpose unless: the individual has consented to its use; it is necessary to prevent an imminent threat to life; it is required by law; or it is necessary for the enforcement of the criminal law.[18] There are also similar limits on disclosure of personal information.[19]

The National Privacy Principles

2.10 While the Commonwealth IPPs apply to Australian Government agencies, the National Privacy Principles ("NPPs") apply to private

9. IPP 1.
10. IPP 2.
11. IPP 3.
12. IPP 4.
13. IPP 5.
14. IPP 6.
15. IPP 7.
16. IPP 8.
17. IPP 9.
18. IPP 10.
19. IPP 11.

sector organisations with an annual turnover of over $3million that do not have their own approved privacy codes. An "organisation" is defined as an individual, a body corporate, a partnership, or any other unincorporated association or a trust.[20]

2.11 Amendments to the *Privacy Act* in 2000[21] allowed private sector organisations to develop their own privacy codes, which, once approved by the Privacy Commissioner, would replace the NPPs. To date, there are only three approved and operative codes.[22] Hence, the NPPs continue to have wide application in the private sector.

2.12 The 10 NPPs are contained in Schedule 3 to the *Privacy Act*[23] and regulate collection of information, use and disclosure, data quality, data security, openness, access and correction, identifiers, anonymity, transborder data flows and sensitive information.

A unified set of principles

2.13 The two sets of principles are largely similar, with a few differences. For instance, the NPPs have special rules regarding the handling of sensitive information and the transfer of personal information overseas whereas the Commonwealth IPPs do not. On the other hand, there are some instances when both sets of principles may apply to one organisation, such as when Government services are outsourced to a private organisation.

2.14 The Australian Law Reform Commission ("ALRC"), in its Discussion Paper 72, *Review of Privacy*, has proposed that there should be one set of principles that applies to both the public and private sectors and refers to these new principles as the Unified Privacy Principles.[24] These proposed new principles have been drafted and structured using the NPPs as a template.

2.15 As well as creating a unified set of principles, the ALRC has proposed some changes to the contents of the principles.[25] For instance, it proposes that the principle of anonymity, which is contained in NPP 8, should be extended to apply to agencies (in addition to organisations which are already covered by NPP 8).[26]

---

20. *Privacy Act 1988* (Cth) s 6C.
21. *Privacy Amendment (Private Sector) Act 2000* (Cth).
22. These are: the *Market and Social Research Privacy Code*, the *Queensland Club Industry Privacy Code* and the *Biometrics Institute Privacy Code*. The *General Insurance Information Privacy Code* was approved but has since been revoked.
23. Unlike the IPPs, which are contained in the body of the Act (in s 14).
24. ALRC DP 72, Proposal 15-2, 567.
25. ALRC DP 72, Vol 2, pt D, Ch 15-28.
26. ALRC DP 72, 590-591.

Similarly, the ALRC has proposed that agencies and organisations should have the option to transact pseudonymously provided it is lawful, practicable and not misleading.[27]

2.16 The ALRC also evaluated the need to include additional privacy principles not currently covered by the IPPs or the NPPs, such as an accountability principle, a prevention of harm principle, a consent principle and a data breach notification principle. It ultimately concluded against such inclusion.[28]

Exceptions and exemptions

2.17 The provisions of the *Privacy Act* are subject to a wide range of exemptions, partial exemptions and exceptions that limit the application of the Act. They are scattered throughout the Act in the definitions of terms, in the Commonwealth IPPs and NPPs and in specific exemption/exception provisions.[29]

2.18 The distinction between exemptions, partial exemptions and exceptions is explained in the following paragraphs.

2.19 Exemptions apply to a specified entity or organisation. Small businesses, namely those with an annual turnover of $3million or less, registered political parties, State and Territory authorities and prescribed State and Territory instrumentalities are excluded from the definition of an “organisation”[30] and thus exempt from the operation of the *Privacy Act*.[31] By virtue of s 7 of the *Privacy Act*, the acts and practices of agencies listed under the *Freedom of Information Act 1982* (Cth), a federal court, a Minister, the Integrity Commissioner, the ACC and a Royal Commission are wholly exempted from the operation of the *Privacy Act*.[32] The ALRC has proposed that both these exemptions be removed.[33]

2.20 Partial exemptions are those that apply to a specified entity or a class of entity, but only partially, removing the requirement to comply with some, but not all, of the privacy principles or only apply in relation to particular activities. Thus, even where a certain entity falls within the definition of an “agency” or an “organisation”, their acts and practices may still be exempt from the *Privacy Act* if those acts or

27. ALRC DP 72, 595-597.
28. ALRC DP 72, Chapter 29.
29. For a detailed discussion of exemptions and exceptions see ALRC DP 72, Vol 2, pt E.
30. *Privacy Act 1988* (Cth) s 6C(1), subject to s 6E and s 6EA in the case of small business operators.
31. *Privacy Act 1988* (Cth) s 6D.
32. *Privacy Act 1988* (Cth).
33. ALRC DP 72, Proposals 35-1, 37-1 and 34-5.

practices are excluded from the definition of acts or practices to which the Act applies. For instance, the federal courts fall within the definition of an "agency" but only their administrative matters are covered by the Commonwealth IPPs. Activities of the courts that relate to non-administrative matters are exempt from the *Privacy Act* because they fall outside the definition of an "act or practice".[34]

2.21 In the public sector, there are more than 20 agencies that are partially or completely exempt from the Act.[35] In the private sector, apart from the specifically exempt entities, namely, the small business operators, registered political parties, State and Territory authorities and prescribed State and Territory instrumentalities, there are eight categories of organisations that are exempt from the operation of the Act.[36]

2.22 Exceptions occur where a requirement in the privacy principles does not apply to an entity in specified circumstances or in respect of certain conduct. For instance, an organisation is usually prohibited from using or disclosing information for a secondary purpose. However, an exception to this prohibition lies where an individual has consented to such use or disclosure.[37]

2.23 Some have argued that the many exemptions and exceptions make the *Privacy Act* ineffectual. The merits of this argument have been canvassed by the ALRC,[38] whose view is that "exemptions should be limited to the extent possible and justified on sound policy grounds".[39] The ALRC has made a number of proposals in accordance with this policy position. The ALRC has also recommended streamlining the exemptions and exceptions by grouping them according to categories of applicable entities or types of acts or practices in a separate part of the Act, and setting out exemptions and partial exemptions to specific named entities in a Schedule to the Act.[40]

34. *Privacy Act 1988* (Cth) s 7(1)(a)(ii).
35. *Privacy Act 1988* (Cth) s 7.
36. These are: individuals acting in a non-business capacity (s 7B(1)); contracted service provider for a Commonwealth contract (s 7B (2)); current or former employers of an individual (s 7B(3)); media organisation (s 7B(4)), contracted service providers for a State contract (s 7B(5)); political representatives (s 7C); related bodies corporate (s 13B); partnerships (s 13C).
37. NPP 2.1(b).
38. ALRC DP 72, Ch 30.
39. ALRC DP 72, 892, [30.55].
40. ALRC DP 72, 896-897, Proposals 30-1 and 30-2.

Breaches

2.24 An interference with privacy constitutes a breach of the *Privacy Act*. Part III states that an act or practice by an agency that breaches an IPP,[41] and an act or practice by an organisation that breaches an NPP,[42] are both interferences with privacy. There are various other breaches that are considered interferences with privacy, such as breaches of tax file number guidelines,[43] data matching[44] and credit reporting infringements.[45]

Enforcement

2.25 The *Privacy Act* provides that individuals may complain about any acts or practices by an agency or organisation that may be an interference with privacy but there is no right to direct civil action by individuals against agencies or organisations that breach the *Privacy Act*. The Privacy Commissioner is empowered to investigate, conciliate and make determinations, either dismissing the complaint or finding the complaint substantiated. The only compensation available to complainants is through the Privacy Commissioner's power to make a declaration that a complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint.[46] However, such determinations are not binding between the parties. If it becomes necessary to enforce the determination, action must be taken in the Federal Court or the Federal Magistrates Court.[47] Since the *Privacy Act* commenced, the Privacy Commissioner has made only two determinations awarding compensation for loss or damage.[48]

2.26 The *Privacy Act* also gives the Privacy Commissioner a discretion to refer complaints to other bodies, such as the Human Rights and Equal Opportunity Commission, the Ombudsman, the Postal Industry Ombudsman or the Public Service Commissioner.[49] Where organisations are guided by an approved privacy code, the code

---

41. *Privacy Act 1988* (Cth) s 13.
42. *Privacy Act 1988* (Cth) s 13A.
43. *Privacy Act 1988* (Cth) s 13(b).
44. *Privacy Act 1988* (Cth) s 13(ba).
45. *Privacy Act 1988* (Cth) s 13(d).
46. *Privacy Act 1988* (Cth) s 52(1)(b)(iii).
47. *Privacy Act 1988* (Cth) s 55A.
48. See <http://www.privacy.gov.au/act/casenotes/index.html#comdet> at 1 December 2006. Both cases involved disclosure of personal information by government agencies. The Privacy Commissioner determined $2,643 in one case and $5,000 in the other as appropriate compensation.
49. *Privacy Act 1988* (Cth) s 50.

can provide state the procedures for dealing with complaints that do not involve the Privacy Commissioner.

OTHER FEDERAL PRIVACY LEGISLATION

2.27 There are a number of other federal statutes relating to dealings with personal information. For example, the handling of tax file numbers is regulated by various statutes, such as the *Income Tax Assessment Act 1936* (Cth), the *Taxation Administration Act 1953* (Cth) and the *Data-matching Program (Assistance and Tax) Act 1990* (Cth).[50]

2.28 Other significant federal statutes relating to privacy include the following:

- The *Freedom of Information Act 1982* (Cth) grants every person a right to access documents held by government agencies or Ministers, including information about the person who is seeking access. The Act provides for exemptions, such as documents relating to the national security, defence or international relations, cabinet documents, internal working documents of government agencies and Ministers, documents subject to legal professional privilege, documents affecting personal privacy, and so forth.[51] The Act also gives an individual the right to have personal information relating to him or her amended by the relevant government body.[52] Similar access and amendments rights are provided by the *Privacy Act* and parallel State information privacy statutes. This is the main area of overlap between freedom of information and information privacy statutes.[53]

---

50. There are provisions under other federal legislation that require or authorise certain acts involving the collection, use and disclosure of personal information. For example, the *Census and Statistics Act 1905* (Cth) and the *Commonwealth Electoral Act 1918* (Cth) require or authorise the collection of large amounts of personal information. Other Acts require or authorise the disclosure of personal information in a range of circumstances, such as the *Australian Passports Act 200*5 (Cth), *Corporations Act 2001* (Cth), *Telecommunications Act 1997* (Cth) and *Migration Act 1958* (Cth).
51. See *Freedom of Information Act 1982* (Cth) pt IV (exempt documents). For a recent decision illustrating one class of exempt documents (internal working documents of government agencies or Ministers), see *McKinnon v Secretary, Department of Treasury* [2006] HCA 45.
52. See *Freedom of Information Act 1982* (Cth) pt V (amendment and annotation of personal records).
53. There are at least two areas of potential friction or conflict. The first is where a document subject to protection from disclosure under an information privacy statute is required to be disclosed under freedom of information legislation. The second is where a person who has rights of

- The *Telecommunications (Interception and Access) Act 1979* (Cth) safeguards the privacy of individuals when using the telecommunications system, telephones in particular. The Act makes it an offence to intercept communications passing over the telecommunications system, at the same time balancing Australia's law enforcement and national security interests. It specifies the circumstances in which it is permissible for law enforcement agencies and the Australian Security Intelligence Organisation to intercept communications under the authority of a warrant, subject to reporting and accountability mechanisms.
- The *Australian Postal Corporation Act 1989* (Cth) safeguards the privacy of individuals when using the postal services system. The Act makes it an offence to open or examine articles while they are in the course of post and under the control of Australia Post.[54]

access and amendment under information privacy laws has similar rights which are subject to differently worded exceptions under freedom of information legislation: see M Paterson, *Freedom of Information and Privacy in Australia* (Butterworths, 2005), [1.46]-[1.51].

54. See *Australian Postal Corporation Act 1989* (Cth) pt 7B (dealing with articles and their contents).

3. Current privacy protection – New South Wales

- Introduction
- The Privacy and Personal Information Protection Act 1998 (NSW)
- The Health Records and Information Privacy Act 2002 (NSW)
- Other related New South Wales legislation

INTRODUCTION

3.1 In New South Wales, there are two main statutes that offer privacy protection, principally in relation to the handling of personal information, namely the *Privacy and Personal Information Protection Act 1998* (NSW) ("PPIPA") and the *Health Records and Information Privacy Act 2002* (NSW) ("HRIPA"). This chapter provides a summary of the coverage of each statute, the role and purpose of the information protection principles and the health privacy principles, the applicable exemptions and the complaints handling mechanisms.

3.2 Other New South Wales statutes that regulate aspects of privacy are the *Workplace Surveillance Act 2005* (NSW), *Listening Devices Act 1994* (NSW), *Crimes (Forensic Procedures) Act 2000* (NSW), *Freedom of Information Act 1989* (NSW), *State Records Act 1998* (NSW) and the *Local Government Act 1993* (NSW). These are dealt with in brief in paragraph 3.93.

THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998 (NSW)

3.3 PPIPA is intended "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* (NSW); and for other purposes"[1] and regulates the handling of personal information (excluding health information)[2] by New South Wales public sector agencies. Unlike the *Privacy Act 1988* (Cth), it does not cover the private sector. It defines personal information 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."[3]

1. *Privacy and Personal Information Protection Act 1998* (NSW), Long Title.
2. *Privacy and Personal Information Protection Act 1998* (NSW) s 4A.
3. *Privacy and Personal Information Protection Act 1998* (NSW) s 4(1). The wording is similar to the definition in the *Privacy Act1988* (Cth). However, the main difference between the two definitions is that the New South Wales Act contains a list of exceptions. It excludes from the definition, among other things: information about an individual who has been dead over 30 years; information that is contained in a publicly available publication; and information arising out of various acts such as the *Witness Protection Act 1995* (NSW): *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3).

3.4 It sets out Information Protection Principles ("IPPs") that are similar, but not identical, to the Commonwealth IPPs found in the Commonwealth Act. There are a number of differences between the Commonwealth IPPs and the New South Wales IPPs. For example, in relation to the principle relating to storage and security of personal information, PPIPA provides that the relevant public sector agency must not keep information longer than necessary. Further the agency must ensure secure disposal of personal information, in accordance with retention and disposal requirements.[4] The Commonwealth IPPs are silent on this matter.

Background and development of PPIPA

3.5 PPIPA established the first enforceable standards for the collection, storage, use and disclosure of personal information in the public sector in New South Wales. It replaced the original *Privacy Committee Act 1975* (NSW), which had put New South Wales at the forefront of privacy protection in the world, although it did not contain any enforceable standards. PIPPA was passed in 1998, but commenced in stages, not requiring public sector agencies to be bound by the standards until July 2000.

3.6 The objectives of PPIPA are set out in the Second Reading Speech of the then Attorney General, the Hon Jeff Shaw, QC, as follows:

- 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. *Privacy and Personal Information Protection Act 1998* (NSW) s 129(a) and (b).

3.7 PPIPA has been amended from time to time since its enactment. In 2002, the right of prisoners and their families to receive monetary compensation for breaches of privacy by government agencies was removed.[5] In 2004, other amendments passed in 2002 came into operation. One amendment allowed sensitive personal information to be disclosed only where there is a serious and imminent threat to the life or health of the individual concerned or another person. Another amendment ensured that public sector agencies and personnel who give access to personal information, in good faith, are not liable for those acts.[6] Regulations making transitional arrangements[7] and creating exemptions[8] have also been passed.

3.8 The New South Wales Attorney General's Department conducted a statutory review of PPIPA in 2004. This was in accordance with the legislative requirement that the Act be reviewed five years from its date of commencement to ensure that the policy objectives remained valid and that the provisions in the Act remained appropriate for securing the objectives.[9] The review considered over 70 submissions and in its report made 27 recommendations for reform, many of which are considered in this inquiry.

What is covered?

3.9 While there are many different aspects to privacy protection including the protection of bodily privacy, privacy of personal behaviour, privacy of communications and territorial privacy, PPIPA is primarily concerned with privacy of personal information. This is expansively defined to include an individual's fingerprints, retina prints, body samples or genetic characteristics.[10] If certain information is considered "personal information" under PPIPA, then information privacy focuses on the need to ensure that an individual's personal information is dealt with in a manner that is fair and reasonable. It is

---

5. *Privacy and Personal Information Protection Amendment (Prisoners) Act 2002* (NSW).
6. *Health Records and Information Privacy Act 2002,* Sch 3 contained these and other amendments to the *Privacy and Personal Information Protection Act 1998* (NSW).
7. *Privacy and Personal Information Protection (Transitional) Regulation 1999* (NSW).
8. *Privacy and Personal Information Protection Regulation 2000* (NSW) 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 PPIPA and exempts the Councils of the Law Society and the Bar Association from the operation of PPIPA.
9. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly).
10. *Privacy and Personal Information Protection Act 1998* (NSW) s 4(2).

often confused with secrecy and confidentiality but it is in fact a much broader concept.

3.10 Although PPIPA primarily deals with information privacy, it does have a wider ambit by virtue of the Privacy Commissioner's general power to " receive, investigate and conciliate complaints about *privacy related matters*" [emphasis added].[11] However, the remedy available for breaches of privacy is limited to conciliation. This issue is discussed in detail in Chapter 5.

What is "personal information"?

3.11 As noted above, "personal information" is a key concept in determining the scope of PPIPA and is defined in s 4 to mean any information or opinion about an identifiable person. It includes:

- written records about a person;
- a photograph or image of a person;
- fingerprints or DNA samples that identify a person; and
- information about a person that is not written down, but which is in the possession or control of the agency.

3.12 Privacy NSW is of the view that "personal information" does not always have to include a name. The test is whether a person's identity can reasonably be ascertained from the information or opinion.[12] Thus, the provision of other details may be sufficient to identify a person even if the name is withheld. The name alone, in the absence of any other information, is also often adequate to qualify as personal information in contexts where it implies some further information that would itself qualify as personal information, for instance, the name appearing on a debt recovery list.[13]

3.13 The definition of "personal information" is, however, subject to a wide range of exemptions. Section 4 of PPIPA sets out the range of information that is not to be included within the definition of "personal information" as follows:

> (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

11. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(k).
12. Privacy NSW, *Consultation* (29 June 2007).
13. Privacy NSW, *Consultation* (29 June 2007).

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 Act 1990*,

(i) information about an individual that is contained in a document of a kind referred to in clause 1 or Schedule 1(restricted documents) to the *Freedom of Information Act 1989* (ie Cabinet or Executive Council documents),

(j) information or an opinion about an individual's suitability for appointment or employment as a public sector official,

(ja) information about an individual that is contained about an individual under Chapter 8 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.

This dramatic cutting back of what constitutes personal information by virtue of the number of exemptions is analysed in Chapter 5.[14]

Who is covered?

3.14 PPIPA deals with management of information privacy by all public sector agencies, defined in s 3 to include: all State government departments, statutory or declared authorities, the NSW Police service, local councils and bodies whose accounts are subject to the Auditor General.

3.15 Section 3 specifically excludes State owned corporations from the definition of "public sector agency". The rationale for this exclusion was originally to ensure that they would not have to comply with privacy principles that equivalent private sector organisations were not required to comply with. Subsequently however, the federal privacy legislation was extended to apply to the private sector and

14. See para 5.7-5.50.

state instrumentalities were required to be incorporated under the *Corporations Act 2001* (Cth) or be specifically prescribed for the *Privacy Act 1988* (Cth) to be applicable. To date, only four New South Wales State owned corporations have been prescribed. The question of whether State owned corporations should continue to be excluded from the operation of PPIPA is explored in Chapter 5.

3.16 There are further provisions strewn through PPIPA that exempt many agencies and entities from the operation of the Act. For instance, s 27 of PPIPA exempts law enforcement agencies, namely the Independent Commission Against Corruption, the Police Service, the Police Integrity Commission, the Inspector of the Police Integrity Commission, the staff of the Inspector of the Police Integrity Commission and the NSW Crime Commission, from the requirement to comply with the IPPs, which effectively covers the scope of PPIPA. While the rationale for this exemption was to ensure that "the purpose of the legislation is not to protect secrecy in dealings or to protect the Government from accountability for its actions",[15] Privacy NSW is concerned that there are negative side effects of such exemptions.[16] This issue is canvassed in detail in Chapter 5.

3.17 There are many other similar limitations to the scope and operation of PPIPA, discussed in detail in Chapter 5.

The Information Protection Principles

3.18 Sections 8-19 set out 12 Information Protection Principles (IPPs), described as the "backbone" of PPIPA, that must be adhered to by all public sector agencies in the management of personal information. These principles can be grouped into five main categories according to the areas they regulate:

- collection;
- storage;
- access;
- use; and
- disclosure.

3.19 **Collection** of information is dealt with in IPPs 1-4,[17] which require that collection must be:

---

15. New South Wales, *Parliamentary Debates*, Legislative Council, 17 September 1998, 7599-7602 (the Hon J W Shaw).
16. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1988* (24 June 2004), 72.
17. *Privacy and Personal Information Protection Act 1998* (NSW) s 8-11.

1. for a lawful purpose and only if it is directly related to the agency's activities and necessary for that purpose;[18]

2. collected directly from the person concerned, unless the person concerned has given consent to obtain the information from another person or the person concerned is a minor (in which case, parents and guardians can give consent);[19]

3. collected in an open manner in that before collecting personal information, agencies must inform the person of the actual collection, the purpose/s of collection, the intended recipients, whether the supply of information is required by law or is voluntary, whether the person can have access to and correct the information;[20] and

4. relevant, accurate, up to date, complete and not excessive.[21]

3.20 **Storage** of information is dealt with in IPP 5:

5. Agencies must ensure that the information is stored securely and that it is not kept for longer than is necessary. When the information is disposed of, such disposal must also be done appropriately. [22]

3.21 **Access** to information is dealt with in IPPs 6-9:

6. All reasonable steps must be taken to enable a person to ascertain what information is being stored, the purpose of storage and any rights the person may have to access the information,[23] with a view to ensuring transparency.

7. The information held by an agency must also be accessible at the request of the person concerned, and must be provided without unreasonable delay or expense. [24]

8. The agency must, at the request of the person concerned, make necessary amendments to the information to ensure that the information is accurate, relevant and up to date, complete and not misleading.[25]

3.22 **Use** of information is dealt with in IPPs 9 and 10:

---

18. *Privacy and Personal Information Protection Act 1998* (NSW) s 8.
19. *Privacy and Personal Information Protection Act 1998* (NSW) s 9.
20. *Privacy and Personal Information Protection Act 1998* (NSW) s 10.
21. *Privacy and Personal Information Protection Act 1998* (NSW) s 11.
22. *Privacy and Personal Information Protection Act 1998* (NSW) s 12.
23. *Privacy and Personal Information Protection Act 1998* (NSW) s 13.
24. *Privacy and Personal Information Protection Act 1998* (NSW) s 14.
25. *Privacy and Personal Information Protection Act 1998* (NSW) s 15.

9. Agencies must ensure that the information is accurate before using it.[26]

10. The information can only be used for the limited purpose for which it was collected, for a directly related purpose, or for a purpose to which consent has been given. It can also be used without consent in order to deal with a serious and imminent threat to a person's health or safety.[27]

3.23 **Disclosure** of information is dealt with in IPPs 11 and 12:

11. Disclosure is restricted to information with consent or for a related purpose that is unlikely to be objected to. Disclosure without consent is only permitted in order to deal with a serious and imminent threat to any person's health or safety.[28]

12. Sensitive information is safeguarded and can only be disclosed with consent or without consent to deal with a serious and imminent threat to any person's health or safety.[29]

Exemptions

3.24 The exemption mechanism that applies to information privacy is fourfold:

- exemptions within PPIPA;
- exemptions effected by regulations;
- exemptions in privacy codes of practice, made by the Attorney General under PPIPA; and
- exemptions in public interest directions, made by the Privacy Commissioner under PPIPA.

Exemptions within PPIPA

3.25 The exemptions in PPIPA are contained in various parts of the Act and apply to various aspects of its coverage. Division 3 of Part 2 deals with specific exemptions from the IPPs. Some exemptions apply in relation to all IPPs,[30] while others limit the operation of particular IPPs.[31]

3.26 Exemptions also arise out of the definitions. For instance, as stated above, the definition of a "public sector agency" specifically

26. *Privacy and Personal Information Protection Act 1998* (NSW) s 16.
27. *Privacy and Personal Information Protection Act 1998* (NSW) s 17.
28. *Privacy and Personal Information Protection Act 1998* (NSW) s 18.
29. *Privacy and Personal Information Protection Act 1998* (NSW) s 19.
30. *Privacy and Personal Information Protection Act 1998* (NSW) s 22.
31. *Privacy and Personal Information Protection Act 1998* (NSW) s 23.

excludes State owned corporations from its operation,[32] just as the definition of "personal information" excludes a range of information in 12 different circumstances.[33]

3.27 There are also various investigative agencies that are specifically exempted from the operation of PPIPA, such as the Independent Commission Against Corruption, the NSW Police Force and the NSW Crime Commission.[34] Other organisations, such as the Ombudsman's Office, the Health Care Complaints Commission, the Anti-Discrimination Board and the Guardianship Board, are exempted from the application of a particular IPP relating to sensitive information.[35]

3.28 Yet another category of exemption applies to courts, tribunals and Royal Commissions but only in respect of their respective judicial and Commission functions.[36]

3.29 Section 5 of PPIPA exempts the *Freedom of Information Act 1989* (NSW) from its ambit while s 20(5) imports restrictions from the *Freedom of Information Act* into PPIPA. However, there appears to be some concern over the practical application of these provisions and the relationship between privacy and access to information. This is discussed in detail in Chapter 6 at paragraph 6.32 and in Chapter 8 at paragraph 8.10. Similarly, the *Local Government Act 1993* (NSW) makes provision for access to information giving rise to possible competing statutory requirements between PPIPA and the *Local Government Act 1993* (NSW). The interaction between privacy and access to information is dealt with in Chapter 7.

Other exemption mechanisms - regulations, codes and directions

3.30 PPIPA also establishes mechanisms, namely regulations, codes and directions, by which exemptions are made.

3.31 ***Regulations***. Section 71 makes provision for the Governor to make regulations exempting specified persons or public sector agencies from any of the provisions of PPIPA. The *Privacy and Personal Information Protection Regulation 2005* exempts:

---

32. *Privacy and Personal Information Protection Act 1998* (NSW) s 3.
33. *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3). See para 3.13.
34. *Privacy and Personal Information Protection Act 1998* (NSW) s 27.
35. *Privacy and Personal Information Protection Act 1998* (NSW) s 28.
36. *Privacy and Personal Information Protection Act 1998* (NSW) s 6.

- certain information contained in archives, or held by a library, art gallery or museum or the State Records Authority from the definition of personal information;
- certain public sector agencies from the requirements of s 33 to prepare and implement a privacy management plan;[37]
- certain public registers and rolls kept by: the Registrar General under the *Real Property Act 1900* (NSW) and the *Conveyancing Act 1919* (NSW); the Valuer General; the Attorney General with respect to the register of justices; and the Minister administering the *Water Management Act 2000* (NSW) from the provision of Part 6 of PPIPA; and [38]
- the Law Society and the Bar Association from the operation of PPIPA generally.[39]

3.32 ***Privacy codes***. Part 3 of Division 1 provides for the making of privacy codes of practice by an order of the Attorney General in consultation with the Privacy Commissioner. This differs from the making of regulations, which require no consultation with the Privacy Commissioner, but can be disallowed by Parliament. Privacy codes are made "for the purpose of protecting the privacy of individuals"[40] and "may regulate the collection, use and disclosure of, and the procedures for dealing with, personal information held by public sector agencies".[41] Section 30 states that a privacy code may modify IPPs and in particular, may:

> (a) specify requirements that are different from the requirements set out in the principles, or exempt any activity or conduct of or by the public sector agency from compliance with any such principle, and
>
> (b) specify the manner in which any one or more of the information protection principles are to be applied to, or are to be followed by, the public sector agency, and
>
> (c) exempt a public sector agency, or class of public sector agency, from the requirement to comply with any information protection principle.

3.33 The Attorney General has approved a number of privacy codes of practice that modify or waive the application of the IPPs. An issue arising out of the scope of privacy codes is raised in Chapter 7 at paragraphs 7.12-7-13.

---

37. *Privacy and Personal Information Protection Regulation 2005* (NSW) cl 5.
38. *Privacy and Personal Information Protection Regulation 2005* (NSW) cl 6.
39. *Privacy and Personal Information Protection Regulation 2005* (NSW) cl 7.
40. *Privacy and Personal Information Protection Act 1998* (NSW) s 29(1).
41. *Privacy and Personal Information Protection Act 1998* (NSW) s 29(2).

3.34 ***Directions***. The Privacy Commissioner may make a written direction approved by the Attorney General exempting agencies from complying with IPPs or privacy codes or may direct that an IPP or code is modified as specified.[42] Such directions are referred to as "public interest directions" because the Privacy Commissioner must be satisfied that the public interest in requiring the public sector agency to comply with the principle or code is outweighed by the public interest in making the direction. While such directions are intended as short-term solutions to problems complying with a code or principle, the danger is that they remain in operation.

Enforcement

3.35 Section 53 of PPIPA states that "a person who is aggrieved by the conduct of a public sector agency is entitled to a review of that conduct". Thus, if a complaint is about personal information and against a New South Wales public sector agency, the aggrieved person could seek an internal review of the complaint.

3.36 Enforcement of the privacy principles set out in PPIPA is therefore primarily through administrative review where individual applicants may seek internal review of the conduct or a decision. This process could result in binding findings and enforceable remedies available on subsequent application to the Administrative Decisions Tribunal. However, there are few applications filed and fewer decisions made, with the majority being resolved by alternative dispute resolution processes.[43]

3.37 PPIPA also aims to protect "the privacy of individuals generally". Section 45(1) states that "a complaint may be made to (or by) the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual."

3.38 Section 45(2) provides that the subject matter of a complaint may relate to conduct to which the alternative process of administrative review applies, implying that its scope is broader than the breach of the IPPs by a public sector agency. Thus, if the complaint is about physical privacy and against an organisation that is not a public sector agency, the person can make a complaint to Privacy NSW.

3.39 Although the Privacy Commissioner may investigate any complaint about an alleged violation or interference with the privacy

---

42. *Privacy and Personal Information Protection Act 1998* (NSW) s 41.
43. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (26 May 2004).

of an individual, even those that go beyond the conduct of the New South Wales public sector agencies and a breach of the IPPs, it would appear that the focus is on the individual complainant, rather than investigation and resolution of systemic privacy issues.[44]

3.40 While there are two avenues for complaint resolution under PPIPA, there is no requirement that complainants make a choice. Indeed, s 45 allows the Privacy Commissioner to accept complaints that could also be the subject of the internal review mechanism.[45] This was clearly the intention of the provision as stated by the then Attorney General in the second reading speech:

> … in cases in which the complaint relates to a breach of a data protection principle, relevant code, or breaches of the public register provisions, the complainant can choose to have the Commissioner conciliate the matter or alternatively to seek an internal review by the agency with a right of review by the Administrative Decisions Tribunal.[46]

3.41 However, in practice it appears that the Privacy Commissioner does ask complainants to choose which method they prefer, that is, administrative review process or complaints to the Commissioner.[47] In any event, given the six month time limit within which an internal review application must be lodged, it is unlikely that an applicant can have the benefit of an investigation by the Privacy Commissioner before seeking an internal review. Each of the review mechanisms is discussed below.

Administrative review process via internal review

3.42 Section 53(2) provides that an internal review is to be undertaken by the public sector agency concerned. It is an internal investigation to assess whether or not the complaint is justified, that is, whether or not the agency has complied with its privacy obligations set out in the IPPs. It is conducted by an employee or officer of the agency but not by the individual involved in the subject of the application, and is overseen by Privacy NSW on the application of the aggrieved person. Alternatively, the internal review can be conducted by Privacy NSW on behalf of the agency.[48] If the internal review is conducted by the agency, Privacy NSW is entitled to make submissions to the agency in relation to the subject matter of the

---

44. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998,* [14.10].
45. *Privacy and Personal Information Protection Act 1998* (NSW) s 45(2).
46. New South Wales, *Parliamentary Debates*, Legislative Council, 17 September 1998, 7599-7602 (the Hon J W Shaw).
47. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1988*, 107.
48. *Privacy and Personal Information Protection Act 1998* (NSW) s 54(3).

application.[49] Crucial to the process is that the application for review must be lodged at an office of the public sector agency within six months of the date when the applicant first became aware of the conduct complained of.[50]

3.43 Following the review, the agency may choose to take no further action or may do one or more of the following:

- make a formal apology;
- take remedial action, such as the payment of compensation;
- provide an undertaking that the conduct will not be repeated; and/or
- implement administrative measures to ensure that the conduct is not repeated.[51]

3.44 If the internal review is not completed within 60 days,[52] or if the applicant is dissatisfied with the findings or the action taken, the applicant may apply to the Administrative Decisions Tribunal ("ADT") for a review of the conduct that was the subject of the internal review.[53] The ADT must notify the Privacy Commissioner of any such application and the Commissioner has the right to appear and be heard in any such proceedings.[54]

3.45 On reviewing the conduct of the agency, the ADT can make binding orders requiring, for example, that the agency change its practices, apologise to the complainant or pay damages by way of compensation. Compensation only applies in limited circumstances, such as if the applicant has suffered loss or damage as a result of the conduct.[55] It does not apply where the conduct occurred while the applicant was a convicted inmate.[56]

3.46 A party to the proceedings may appeal to an Appeal Panel of the Tribunal against a decision or order of the Tribunal.[57]

Complaints to the Privacy Commissioner

3.47 Among the functions of the Privacy Commissioner listed in s 36(2) are the functions to "receive, investigate and conciliate complaints about privacy related matters (including conduct to which

---

49. *Privacy and Personal Information Protection Act 1998* (NSW) s 54(2).
50. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(3)(d).
51. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(7).
52. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(6).
53. *Privacy and Personal Information Protection Act 1998* (NSW) s 55.
54. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(6) and (7).
55. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(4).
56. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(4A).
57. *Privacy and Personal Information Protection Act 1998* (NSW) s 56.

Part 5 applies)"[58] and to "conduct such inquiries, and make such investigations, into privacy related matters as the Privacy Commissioner thinks appropriate."[59] In relation to such complaints, s 45(1) states that "a complaint may be made about the alleged violation of, or interference with, the privacy of an individual". Chapter 7 at paragraph 7.21 raises the issue that there is some ambiguity about who may make the complaint that may require clarification.

3.48 Section 45(2) provides that the subject matter of a complaint *may* relate to conduct to which the internal review process applies, implying that a complaint may be made about other privacy related matters. This interpretation is supported by s 46(2), which provides that *if* the complaint relates to conduct for which the internal review process is available, the Privacy Commissioner must inform the complainant of the review process and the remedial action available under that process.

3.49 Sections 45-51 of PPIPA set out the Privacy Commissioner's complaints handling powers. These are:

- inquiry and investigation (with the powers, authorities, protections and immunities available to a Royal Commissioner);
- conciliation; and
- reporting (including reporting to Parliament) on any matter pertaining to the privacy protection of individuals.

3.50 Once the Privacy Commissioner has conducted a preliminary assessment, he or she may decide not to deal with a complaint because: the complaint is frivolous; it is exempted; there are other means of redress; or it would be more suitably dealt with by the internal review process.[60] The Privacy Commissioner may also choose to refer the matter to other authorities for resolution.[61] Even if the Privacy Commissioner declines to deal with a complaint or refers it to another authority for resolution, he or she may still conduct an inquiry or investigation into any general issues or matters raised in connection with the complaint.[62]

3.51 If, however, the Privacy Commissioner decides to deal with the matter, he or she must endeavour to resolve the complaint by conciliation.[63] The Privacy Commissioner may make such inquiries

58. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(k).
59. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(j).
60. *Privacy and Personal Information Protection Act 1998* (NSW) s 46(3).
61. *Privacy and Personal Information Protection Act 1998* (NSW) s 47.
62. *Privacy and Personal Information Protection Act 1998* (NSW) s 51.
63. *Privacy and Personal Information Protection Act 1998* (NSW) s 49(1).

and investigations as appropriate[64] and may request the complainant and the respondent to appear in the proceedings.[65] The Privacy Commissioner may make a written report on findings and recommendations in relation to the complaint.[66]

3.52 Determining whether a particular complaint is a breach of PPIPA, that is, whether it is a "violation or interference with the privacy of an individual", is somewhat difficult in the case of complaints in relation to forms of privacy other than information privacy, as PPIPA provides no specific guidance in this regard. While the relevant standards for assessing a complaint about information privacy against a public sector agency would be the IPPs and the public register provisions, Privacy NSW uses the standards set out in the Complaints Handling Protocol available on their website to determine the validity of other complaints.[67] This aspect of PPIPA's privacy protection is discussed in detail in Chapter 5.

3.53 Complaints to the Commissioner do not give rise to enforceable remedies in that the Commissioner does not have the power to make binding orders or recommendations. In exceptional circumstances, the Commissioner can make a special report to Parliament on the findings of an investigation.

THE HEALTH RECORDS AND INFORMATION PRIVACY ACT 2002 (NSW)

Historical background

3.54 In December 2000, the NSW Ministerial Advisory Committee on Privacy and Health Information presented a report entitled *Panacea or Placebo* to the New South Wales Government. The central recommendation of this report was that personal health information required specific statutory protection. Accordingly, the *Health Records and Information Privacy Act 2002* (NSW) ("HRIPA) was passed in September 2002 and commenced on 1 September 2004, establishing "a comprehensive regime for the management and protection of health information across both the private and public sectors in New South Wales".[68]

---

64. *Privacy and Personal Information Protection Act 1998* (NSW) s 48(1)(b).
65. *Privacy and Personal Information Protection Act 1998* (NSW) s 49(2).
66. *Privacy and Personal Information Protection Act 1998* (NSW) s 50(1).
67. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1988*, 103.
68. New South Wales, *Parliamentary Debates*, Legislative Council, 11 June 2002, Second Reading Speech, 2958-2959 (Michael Egan).

3.55 HRIPA protects the privacy of an individual's health information.[69] It does this by requiring those who handle health information in both the public and private sectors to comply with 15 Health Privacy Principles.[70] Coverage of the private sector is possibly the most notable distinction between PPIPA and HRIPA, although the protection afforded is limited to health information.

3.56 As HRIPA was passed several years after PPIPA, it was drafted with the benefit of experience of, and hindsight into, the operation of privacy laws in New South Wales. As noted in the Second Reading Speech, the development of HRIPA was guided by three principles:

> The first is to recognise obligations already imposed on service providers and health service providers by the existing laws, such as the Federal Privacy Act.
>
> The second principle is to draw together the best elements of existing privacy legislation at a local, national and international level. In this regard, particular attention has been given to the obligations currently imposed on the public sector in New South Wales under the Privacy and Personal Information Protection Act, as well as the reforms recently introduced in Victoria in the Health Records Act. The experience to date in other jurisdictions has been useful to the development of this bill. It reinforces the need for a flexible and adaptive legislative scheme capable of accommodating the complexities arising in the management of health information.
>
> The third principle is the aim to ensure a readily accessible and usable set of principles having due regard to both individual rights and the special needs arising in the management and use of health information. In this regard the bill endeavours to strike an appropriate balance between the desire of consumers for privacy on the one hand, and the need to safeguard the health and safety of individuals and

---

69. The Act defines health information as personal information or an opinion about an individual's physical or mental health or disability, an individual's express wishes about the future provision of health services to him or her, or a health service provided to an individual. It also includes other personal information collected in providing a health service, or other personal information about an individual collected in connection with the donation of an individual's body parts, organs or body substances. Further, it includes genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health of the individual or any of his or her siblings, relatives or descendants: *Health Records and Information Privacy Act 2002* (NSW) s 6.
70. See *Health Records and Information Privacy Act 2002* (NSW) Sch 1.

> the public, and promote safe and effective health service delivery on the other.[71]

3.57 The purpose of HRIPA, as set out in s 3, is to:

> promote fair and responsible handling of health information by:
>
> (a) protecting the privacy of an individual's health information that is held in the public and private sectors, and
>
> (b) enabling individuals to gain access to their health information, and
>
> (c) providing an accessible framework for the resolution of complaints regarding the handling of health information.

3.58 The objects are:

> (a) to balance the public interest in protecting the privacy of health information with the public interest in the legitimate use of that information, and
>
> (b) to enhance the ability of individuals to be informed about their health care, and
>
> (c) to promote the provision of quality health services.

3.59 While there are still areas that warrant improvement and reform, HRIPA is considered a significant improvement on other existing privacy legislation, both structurally and in terms of achieving its objects.[72]

What is covered?

3.60 "Health information" is defined in s 6 to be a particular type of personal information, as set out in paragraph 3.61 below. Section 5 of HRIPA defines personal information in similar terms to the definition in PPIPA, although with four further exclusions from the definition. These are:

> (c) 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,
>
> (d) 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;
>
> (e) information about an individual that is contained in the archives within the meaning of the *Copyright Act 1968* of the Commonwealth,

71. New South Wales, *Parliamentary Debates*, Legislative Council, 11 June 2002, Second Reading Speech, 2958-2959 (Michael Egan).
72. See discussion in Ch 4 and 5.

> (n) information about an individual that forms part of an employee record (within the meaning of the *Privacy Act 1988* of the Commonwealth about the individual held by a private sector person.

3.61 Section 6 of HRIPA defines "health information" to mean personal information or an opinion about:[73]

- a person's physical or mental health or disability;
- a person's express wishes about the future provision of health services for themselves;
- other personal information collected to provide, or in providing a health service;
- other personal information about an individual collected in connection with the donation of human tissue or body parts;
- other personal information, such as genetic information about a person arising from a health service provided to them that predicts or could predict the health of that person or of their siblings, relatives or descendants and personal information which has been collected to provide or personal information collected in providing a health service.

3.62 A health service, whether provided as public or private services, is defined in s 4 to include:

> (a) medical, hospital and nursing services;
>
> (b) dental services;
>
> (c) mental health services;
>
> (e) pharmaceutical services;
>
> (f) community health services;
>
> (g) health education services;
>
> (h) welfare services required to implement the services referred to above;
>
> (i) services provided by podiatrists, chiropractors, osteopaths, optometrists, physiotherapists, psychologists and optical dispensers in the course of providing health care;
>
> (j) services provided by dietitians, masseurs, acupuncturists, occupational therapists, speech therapists, audiologists, audiometrists and radiographers in the course of providing health care;

---

73. "Health information" "does not include health information, or a class of health information contained in a class of documents, that is prescribed as exempt health information for the purposes of [the] Act generally or for the purposes of specified provisions of [the] Act".

(k) services provided in other alternative health care fields in the course of providing health care;

(l) a service prescribed by the regulations as a health service for the purposes of this Act.

3.63 A "health service provider" is an organisation that provides health services, as defined above, unless exempted by the regulations. An "organisation" is defined as "a public sector agency or a private sector person". A "private sector person" is defined to mean: a natural person; a body corporate; a partnership; or a trust or any other unincorporated association or body; but does not include a "small business operator".[74] Section 11 provides that the "Act applies to every organisation that is a health service provider or that collects, holds or uses health information".

3.64 Thus, the health service providers regulated by HRIPA range from individual GPs and partnerships of practitioners such as physiotherapists, through to large private and public hospitals and larger organisations that handle health information and have an annual turnover of more than $3million, such as insurance companies that deal with health information.

The Health Privacy Principles

3.65 The key to the operation of HRIPA are the 15 Health Privacy Principles ("HPPs"), which are the legal obligations describing what New South Wales public and private sector organisations must do when they collect, hold, use and disclose health information. Whereas the IPPs are contained in the body of PPIPA, the HPPs are contained in Schedule 1 to HRIPA and are, as a result, easier to identify.

3.66 The 15 HPPs can be grouped into 7 categories according to the areas they regulate:

- collection;
- storage;
- access;
- use;
- disclosure;
- identifiers and anonymity; and
- transferrals and linkage.

3.67 In addition to the HPPs listed above, Part 4 of HRIPA sets out special rules in relation to:

74. *Health Records and Information Privacy Act 2002* (NSW) s 4(1).

- the retention of health information by health service providers;[75]
- providing access to information;[76] and
- amending health information.[77]

These special rules are additional to, and are meant to assist with the operation of, the general HPPs and are discussed below within the context of the relevant HPPs.

3.68 **Collection** of information is dealt with in HPPs 1-4. As is the case with the IPPs,[78] collection of health information must be for a **lawful** purpose and must be directly related to the organisation's activities and reasonably necessary for that purpose. [79] The information collected must also be **relevant** to that purpose, accurate and up to date. It must not be excessive and should not intrude unreasonably on the personal affairs of the individual to whom the information relates.[80] Collection must also be done in an **open** manner where agencies must inform the person concerned of the identity of the organisation collecting the information, the purpose of collection, its use, and so forth.[81] An organisation must collect the health information **directly** from the individual concerned, unless unreasonable or impracticable to do so.[82] This differs from IPP 2, which allows for consent to be given to the collection of information from a third party.

3.69 **Storage** is dealt with in HPP 5. As for IPP 5, health information must be stored securely, not kept for any longer than is necessary and protected from unauthorised access.[83]

3.70 Section 25 of HRIPA (Division 2 of Part 4) contains an additional provision applicable to private sector persons. Private sector health service providers must retain health information collected while the individual was an adult for 7 years from the last occasion on which a health service was provided. In the case of health information collected from a person under the age of 18 years, this must be retained until the person turns 25.

3.71 **Access and accuracy** are dealt with in HPPs 6-9. The organisation holding health information must be **transparent** in

75. *Health Records and Information Privacy Act 2002* (NSW) Part 4 Division 2.
76. *Health Records and Information Privacy Act 2002* (NSW) Part 4 Division 3.
77. *Health Records and Information Privacy Act 2002* (NSW) Part 4 Division 4.
78. See para 3.19.
79. HPP 1: Schedule 1(1).
80. HPP 2: Schedule 1(2).
81. HPP 4: Schedule 1(4).
82. HPP 3: Schedule 1(3).
83. HPP 5: Schedule 1(5).

providing details about what information is being stored, why such information is being stored and what access rights exist.[84] It is also a requirement that such information is **accessible**,[85] **correct**, capable of amendment at the request of the individual to whom the information relates[86] and **accurate**.[87]

3.72 Division 3 of Part 4 (s 26-32) of HRIPA contains additional provisions applicable to private sector persons when an individual requests access to his or her health information. Similarly, Division 4 (s 33-37) makes provision for an individual to request a private sector person to amend that individual's health information.

3.73 **Use** of health information is dealt with in HPP 10. Generally, an organisation can only use information for the purpose for which it was collected or a directly related purpose unless the individual concerned has consented to any other use. There are, however, a range of circumstances when health information may be used for other purposes where necessary, such as: where there is a serious threat to health and welfare; for management of health services, training or research; to find a missing person; investigating suspected unlawful activity; law enforcement; complaint handling or investigative functions; and for circumstances prescribed by the regulations.

3.74 **Disclosure** of health information is dealt with in HPP 11. As with HPP 10, health information cannot be disclosed except for the purpose for which it was obtained or a directly related purpose, unless the individual to whom the information relates has consented. There are similar exceptions to this principle as there are for HPP 10. In addition, an exception is allowed for compassionate reasons.[88]

3.75 **Identifiers and anonymity** are dealt with in HPP 12 and 13. Wherever lawful and practicable, individuals must be entitled to receive health services **anonymously**. An identifier is defined in s 4 of HRIPA to mean something (usually a number) that an organisation assigns to a person in order to uniquely identify that person, such as a person's Medicare number. An organisation can only provide an identification number if it is reasonably necessary to enable the organisation to carry out its functions efficiently. A private sector person may adopt an identifier assigned to an individual by a public sector agency only if the individual has consented to such use or such use is required or authorised by law. Similarly a private sector person may use or disclose such an identifier only in exceptional

84. HPP 6: Schedule 1(6).
85. HPP 7: Schedule 1(7).
86. HPP 8 Schedule 1(8).
87. HPP 9 Schedule 1(9).
88. *Health Records and Information Privacy Act 2002* (NSW) sch 1(11)(1)(g).

circumstances. While there are great benefits for efficient record management in assigning numbers or other identifiers, they also pose a major privacy risk. This is discussed in greater detail in Chapter 6 at paragraphs 6.66-6.71.

3.76 **Transferrals and linkage** are dealt with in HPPs 14 and 15. An organisation must not **transfer** health information about an individual to any person or body outside New South Wales or to a Commonwealth agency unless the individual consents to the transfer, or other specified circumstances exist.[89] An organisation must not include health information about an individual in a health records linkage system (which is a computerised system designed to link health records) unless the individual has expressly consented to the information being included. Again, exceptions to this principle are available if the organisation is lawfully authorised not to comply with the principle or where non-compliance is otherwise permitted.[90]

Consent

3.77 Consent is a crucial concept in the operation of HRIPA but it has not been defined. Except for HPPs 4 and 15, which require express consent, it is also unclear from the legislation whether consent, in cases where it is required, ought to be express or implied.

3.78 Under HPP 4, an organisation is not required to comply with the requirement to notify if the individual to whom the information relates has *expressly consented* to the organisation not complying with it.[91] HPP 4 requires an agency to notify the individual of why their health information is being collected, what will be done with it and who else might see it. Fulfilling these notification obligations does not amount to seeking consent and must not be confused with consent.

3.79 Similarly, under HPP 15, an organisation must not include health information about an individual in a health records linkage system unless the individual has *expressly consented* to the information being so included.

3.80 In certain circumstances, the exemption provisions override the requirement for consent, such as where the information is being used for the primary purpose for which it was obtained, or for a directly related secondary purpose or where it is used under lawful authority. Where it is impracticable to obtain consent, such as where a person

---

89. The exceptional circumstances are listed in sch 1(14) (a)–(h).
90. HPP 15 sch 1(15).
91. *Health Records and Information Privacy Act 2002* (NSW) sch 1 cl 4(4).

lacks capacity to consent, HRIPA makes provision for an authorised representative to act on his or her behalf.[92]

Exemptions

3.81 Like the exemptions to PPIPA, there are four major sources of exemptions to HRIPA. They are:

(a) exemptions within HRIPA;

(b) exemptions effected by regulation;

(c) exemptions in health privacy codes of practice made by the Minister of Health under HRIPA;

(d) exemptions in health public interest directions made by the Privacy Commissioner under HRIPA.

3.82 ***Exemptions within HRIPA***. There are many exemptions within HRIPA, which limit the seemingly wide ambit of the Act. Some are couched within the definitions of terms, others are stated specifically, still others are contained within the HPPs.

3.82 As explained in paragraph 3.13 above, the definition of "personal information" (of which "health information" is a particular type) is subject to a large number of exemptions in s 5(3), thereby limiting the ambit of "health information". There are also exemptions that limit the general operation of the Act. For instance, s 13 provides that nothing in HRIPA affects the manner in which a court or tribunal exercises the court's or tribunal's judicial functions.

3.83 HPPs 1-4, 10, 11 and 14 are not applicable to the collection, use or disclosure of health information by a news medium, if the collection, use or disclosure is in connection with its news activities.[93] Nor do HPPs 6-8 and Part 4 apply to health information held by a news medium in connection with its news activities.[94]

3.84 There are also blanket exemptions whereby HRIPA does not apply to various agencies or organisations. These include: the Independent Commission against Corruption, the Police Service, the Police Integrity Commission and the NSW Crime Commission, except

92. *Health Records and Information Privacy Act 2002* (NSW) s 7 (2).
93. *Health Records and Information Privacy Act 2002* (NSW) s 15(1). "News medium" is defined in s 4 to mean any organisation whose business, or principal business, consists of a news activity.
94. *Health Records and Information Privacy Act 2002* (NSW) s 15(2).

in connection with the exercise of their administrative and educative functions.[95]

Other exemption mechanisms

3.85 As is the case under PPIPA, exemptions can also be effected by regulation, codes of practice or public interest directions by modifying the application of HPPs to particular projects across any number of public or private sector agencies. This may be required where the HPPs have to be balanced against other public interests.

3.86 There is currently only one regulation in force, namely the *Health Records and Information Privacy Regulation 2006*. This exempts organisations taking part in electronic health record pilot programs from the operation of HPP 15 dealing with the linkage of health records. This regulation also exempts Aboriginal Trust Funds Repayment Scheme agencies[96] from the operation of various HPPs.[97] Public sector agencies are also exempt from HPPs 10 and 11 in respect of disclosure of health information to an Aboriginal Trust Funds Repayment Scheme agency.

3.87 The *Health Records and Information Privacy Code of Practice 2005* permits, in certain limited circumstances, the collection, use and disclosure of health information by human services agencies without the consent of the person to whom the health information relates.

3.88 Codes and regulations are drafted by Parliamentary Counsel, while directions made pursuant to s 62 are made by the Privacy Commissioner with the approval of the Minister for Health. Many such directions to modify the application of HPPs have been made but usually only operate for a specified period of time or until the completion of a particular project.[98]

Enforcement

3.89 As stated above, HRIPA covers both the New South Wales public sector agencies as well as the private sector, and as such, both sectors must comply with the 15 HPPs. The private sector must also comply

---

95. See Ch 5 for an analysis of this distinction between functions that are and are not exempt.
96. These include the Department of Aboriginal Affairs, the State Records Authority or the Department of Premier and Cabinet.
97. HPPs 1-4 and 8-11.
98. There are currently three directions that are in force: *Direction relating to the Anti-Social Behaviour Pilot Project*; *Direction on the Incidental Disclosure and the Transfer of Health Information belonging to the (SA) Commission of Inquiry into Children in State Care*; and *Direction relating to the Redfern Waterloo Partnership Project*.

with the additional principles applicable to private sector individuals and agencies in relation to keeping and giving access to health information. A breach of the HPPs or the additional principles will entitle an individual to make a complaint. However, the enforcement process for complaints will depend on whether the complaint is against a public sector agency or a private sector individual or organisation.

3.90 ***Complaints against a private sector person or agency***. Part 6 of HRIPA deals with complaints against the private sector. Section 42 provides that a complaint may be made to the Privacy Commissioner by a private sector person about the alleged contravention of an HPP, a provision of Part 4 or a health privacy code of practice.[99] A complaint must be made in writing within six months of the time when the complainant first became aware of the relevant conduct.[100] On receipt of the complaint, the Privacy Commissioner may conduct a preliminary assessment of the complaint.[101] The Privacy Commissioner may decide not to deal with the complaint if satisfied of one of a number of factors, including that the complaint is vexatious, trivial or exempted conduct.[102] If the Privacy Commissioner is satisfied that there is a prima facie case of a breach of the Act, the Commissioner may:

(a) endeavour to resolve the complaint by conciliation under s 46;

(b) further investigate the complaint and make a report under s 47; or

(c) determine that the complaint has been resolved to his or her satisfaction.[103]

The Commissioner's findings and recommendations are not binding.

3.91 A complainant may apply to the ADT for an inquiry into the complaint, but only if the Privacy Commissioner has made a report pursuant to s 47.[104] The ADT hears the complaint in its original jurisdiction; it does not have jurisdiction to review the Privacy Commissioner's decision.[105] The ADT can make legally binding orders including: an order requiring the respondent to pay the complainant damages not exceeding $40,000; an order requiring the respondent to

99. *Health Records and Information Privacy Act 2002* (NSW) s 42(1).
100. *Health Records and Information Privacy Act 2002* (NSW) s 42(2).
101. *Health Records and Information Privacy Act 2002* (NSW) s 43(1).
102. *Health Records and Information Privacy Act 2002* (NSW) s 43(2).
103. *Health Records and Information Privacy Act 2002* (NSW) s 45.
104. *Health Records and Information Privacy Act 2002* (NSW) s 48.
105. *Health Records and Information Privacy Act 2002* (NSW) note to s 48. See Ch 7 for an analysis of the ADT's jurisdiction in privacy matters.

refrain from any conduct or action in contravention of an HPP; or an order requiring performance of an HPP, a provision of Part 4 or a health privacy code of practice.[106] An order or other decision made by the ADT may be appealed to an Appeal Panel of the ADT.[107]

3.92 ***Complaints against a public sector agency.*** The complaints process in relation to a public sector agency is governed by Part 5 of HRIPA. Thus, where a person is of the view that a public sector agency has breached an HPP, the person can seek an internal review. If the internal review is not completed within 60 days or the person is unhappy with the handling or the results of the internal review, the person can seek a review by the ADT. The ADT can make legally binding orders. If still dissatisfied, the person can appeal to an Appeal Panel of the ADT.

OTHER RELATED NEW SOUTH WALES LEGISLATION

3.93 In addition to PPIPA and HRIPA, the main privacy statutes in New South Wales, there are other statutes that deal with aspects of privacy:

- The *Workplace Surveillance Act 2005* (NSW) prohibits the surveillance by employers of their employees, except where the employer notified the employees about the surveillance, or where the employer has a covert surveillance authority granted by a Supreme Court judge. The forms of surveillance that are regulated by the Act are: camera surveillance; computer surveillance (including the sending and receipt of emails and the accessing of internet websites); and tracking surveillance (such as the use of a Global Positioning System tracking device).[108]

---

106. *Health Records and Information Privacy Act 2002* (NSW) s 54.
107. *Health Records and Information Privacy Act 2002* (NSW) s 57.
108. *Workplace Surveillance Act 2005* (NSW) s 3. There was some doubt as to the continuing operation of the *Workplace Surveillance Act 2005*(NSW) pursuant to s 16 of the *Workplace Relations Act 1996* (Cth) which excluded the operation of State or Territory industrial laws, including an Act of a State or Territory that applies to employment generally and has one or more of its main purposes (among others) regulating workplace relations or providing for the terms and conditions of employment. The High Court upheld the validity of s 16 of the *Workplace Relations Act 1996* (Cth): *NSW v Commonwealth* [2006] HCA 52. It must be noted that industrial relations is currently undergoing significant change with the passage of the *Workplace Relations Amendment (Transition to Forward with Fairness) Act 2008* (Cth). However, the amendments do not appear to impact on s 16 of the *Workplace Relations Act 1996* (Cth) and consequently, the doubt in terms of the operation of the *Workplace Surveillance Act 2005* (NSW) remains unchanged.

- The *Listening Devices Act 1994* (NSW) prohibits the use of a listening device to listen to or record a private conversation, unless such use falls within one of the exceptions specified by the Act, or is authorised by a warrant granted by a judge of the Supreme Court.
- Bodily privacy is dealt with in the *Crimes (Forensic Procedures) Act 2000* (NSW) in the context of DNA testing.
- The *Freedom of Information Act 1989* (NSW) gives every person a right to obtain information held as records by New South Wales government agencies, Ministers, local government and other public bodies. Like its federal counterpart, the Act grants access and amendment rights to an agency's records or documents.[109] The *States Records Act 1998* (NSW) and the *Local Government Act 1993* (NSW) also provide rights of access to New South Wales government records.[110] The relationship between these three Acts and PPIPA is dealt with in Chapter 7.

---

109. See *Freedom of Information Act 1989* (NSW) pt 3 (access to documents), pt 4 (amendment of records).
110. See *States Records Act 1998* (NSW) pt 6 (public access to State records after 30 years); *Local Government Act 1993* (NSW) pt 2 (access to information).

4. Achieving a clear and consistent legislative structure

- Introduction
- Clarifying the structure of New South Wales privacy laws
- Should PPIPA have an objects clause?
- Achieving greater consistency in health information

INTRODUCTION

4.1 Without question, the effectiveness of privacy laws would be optimised through greater clarity and consistency, not only of content, but also of structure. Reducing legislative complexity would inevitably promote ease of understanding and compliance. This is particularly the case with the *Privacy and Personal Information Protection Act 1998* (NSW) ("PPIPA"), which is structurally quite difficult to penetrate.

4.2 Issues of structure are often closely linked to those of scope. As noted in Chapter 5, the major differences between PPIPA and the *Health Records and Information Privacy Act 2002* (NSW) ("HRIPA") are that HRIPA is more narrowly focused than PPIPA in terms of the type of information it regulates, but is broader in its application to both the public and private sectors. These differences in scope account not only for the differences in structure between the two laws, but also help to explain the existence of two separate laws to regulate information privacy in NSW.

4.3 In this chapter, we examine the two main New South Wales privacy laws with a view to proposing structural changes aimed at achieving greater simplicity and harmony. We are also acutely conscious of the problems that arise due to the lack of consistency in privacy legislation at a national, as well as a State, level. Consequently, we have carefully considered the proposals made by the Australian Law Reform Commission ("ALRC") in its current review of Commonwealth privacy laws,[1] and the impact of those proposals on NSW.

4.4 The discussion in this chapter is designed to elicit views on the following key questions:

- Is the structural basis of PPIPA and HRIPA the most effective way of promoting the aims of each piece of legislation?
- Should New South Wales continue, under HRIPA, to regulate the privacy of health information handled by the private sector, given the ALRC's proposal for such information to be regulated nationally?
- If HRIPA is restricted to the regulation of health information held by the public sector only, does the need for separate health privacy legislation in New South Wales persist?

---

1. See Australian Law Reform Commission, *Review of Privacy* (Issues Paper 31, 2006); and Australian Law Reform Commission, *Review of Privacy* (Discussion Paper 72, 2007).

CLARIFYING THE STRUCTURE OF NEW SOUTH WALES PRIVACY LAWS

4.5 During its introduction into New South Wales Parliament in 1998, PPIPA was described as promoting "the protection of privacy and the rights of the individual by the recognition, dissemination and enforcement of data protection principles consistent with international best practice standards".[2] The standards referred to date from the 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.[3] Those Guidelines form the basis of most Australian, and many overseas, information privacy laws.

4.6 As noted in Chapter 3, the regulatory centrepiece of both PPIPA and HRIPA is a series of principles setting out minimum standards for the protection of information privacy. Consequently, both pieces of legislation are generally referred to as being principles-based, rather than rules-based.[4] The main difference between the two forms of regulation lies in the level of detail and proscription, with principles-based legislation focussing more on broad statements of outcomes rather than prohibition of specific conduct.[5] These issues will be discussed in greater detail below.

The structure of PPIPA

4.7 PPIPA consists of eight parts and can broadly be divided into two areas of operation. The first involves the provisions setting out the responsibilities of public sector agencies when dealing with personal information as defined in the Act.[6] The core of this area is the 12 Information Protection Principles ("IPPs"), which establish the minimum standards with which public sector agencies must comply when collecting, storing, handling or disseminating personal information. The IPPs are found in Part 2 of PPIPA.[7] As noted in Chapter 3, they are modelled on, but not identical to, those in the *Privacy Act 1988* (Cth), and apply only to the public sector, with the

---

2. NSW, *Parliamentary Debates*, Legislative Council, 17 September 1998, 7598-99 (the Hon J W Shaw).
3. See «www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html».
4. Although, in reality, both laws represent a hybrid position, containing a mix of principle and rule-based provisions.
5. For a discussion of the differences between principles-based and rules-based legislation, see ALRC DP 72, [15.21]-[15.40].
6. See *Privacy and Personal Information Protection Act 1998* (NSW) s 4.
7. See *Privacy and Personal Information Protection Act 1998* (NSW), pt 2, div 1, s 8-19.

exception of State owned corporations.[8] PPIPA provides for a number of exemptions from compliance with the IPPs.[9]

4.8 Public sector agencies must develop privacy management plans outlining how the IPPs that apply to their organisation are to be implemented. Agencies, or the Privacy Commissioner, may also develop codes of practice that can modify the application of the IPPs, or even provide exemptions. The codes must be approved by the Privacy Commissioner and are made by the Attorney General upon publication in the Government Gazette. The code and management plan provisions are contained in Part 3 of the Act.

4.9 Part 5 sets out the enforcement procedures that may apply where it is alleged that a public sector agency has breached the IPPs or a relevant code of practice, or has breached the provisions concerning public registers contained in Part 6.[10] Complainants may seek redress by requiring the public sector agency concerned to conduct an internal review.[11] If not satisfied with the outcome of the internal review, a complainant may apply to the Administrative Decisions Tribunal for a determination.[12]

4.10 The second area of operation relates to the more general role and functions of the Office of the Privacy Commissioner. The exercise of these functions is not restricted to the public sector or to personal information. Part 3 established the office of the Privacy Commissioner and sets out its educative and investigative functions, together with the role of the Commissioner in dealing with privacy-related complaints.[13] This part of PPIPA operates broadly, since a complaint may be made in relation to any violation of individual privacy.[14]

4.11 Part 7 establishes the Privacy Advisory Committee, comprising the Privacy Commissioner and six members of New South Wales Parliament.[15] The Committee's functions are to advise on matters relevant to the Privacy Commissioner's functions, including recommending material to be contained in guidelines issued by the Privacy Commissioner, and to advise the Attorney General on any

---

8. See Ch 3 for a discussion of which public sector agencies are covered by the *Privacy and Personal Information Protection Act 1998* (NSW).
9. The exemptions from the operation of all or part of the *Privacy and Personal Information Protection Act 1998* (NSW) are discussed in more detail in Ch 3 and 5.
10. See *Privacy and Personal Information Protection Act 1998* (NSW) s 52.
11. *Privacy and Personal Information Protection Act 1998* (NSW) s 53.
12. *Privacy and Personal Information Protection Act 1998* (NSW) s 55.
13. *Privacy and Personal Information Protection Act 1998* (NSW) pt 4, div 2 and 3.
14. *Privacy and Personal Information Protection Act 1998* (NSW) s 45(1).
15. *Privacy and Personal Information Protection Act 1998* (NSW) s 60.

matters referred to the Committee.[16] Part 8 prescribes offences concerning corrupt disclosure and use of personal information by a public official,[17] offering to supply unlawfully disclosed information,[18] and other dealings with the Privacy Commissioner,[19] as well as other miscellaneous provisions.

4.12 PPIPA also provides for exemptions from the requirement to comply with all or part of the Act. Exemptions may relate to certain types of information, particular agencies or classes of agencies, or specific functions of agencies. The exemptions may be expressly included in PPIPA itself,[20] provided for in regulations[21] or a code of practice made by the Attorney General,[22] or included in a public interest direction made by the Privacy Commissioner.[23]

The structure of HRIPA

4.13 In contrast to the 12 IPPs in PPIPA, HRIPA contains 15 Health Privacy Principles ("HPPs") that apply to public and private sector agencies and organisations that collect or handle health information.[24] The HPPs are not located in the body of the Act itself, but in Schedule 1 to HRIPA. As well as regulating data collection,[25] storage and security,[26] and use and disclosure of information,[27] the HPPs deal with accuracy,[28] access to and alteration of data,[29] the assignment of unique identifiers,[30] anonymity,[31] transborder data flows[32] and linkage of

---

16. *Privacy and Personal Information Protection Act 1998* (NSW) s 61.
17. *Privacy and Personal Information Protection Act 1998* (NSW) s 62.
18. *Privacy and Personal Information Protection Act 1998* (NSW) s 63.
19. *Privacy and Personal Information Protection Act 1998* (NSW) s 68.
20. The exemptions are not located in one place, but appear throughout the legislation: see, for example, *Privacy and Personal Information Protection Act 1998* (NSW) s 3, 4, 4A, 6, 20 and s 23-28, as well as exceptions to each IPP specified in s 8-19.
21. For example, the *Privacy and Personal Information Protection Regulation 2005* (NSW).
22. Made under the *Privacy and Personal Information Protection Act 1998* (NSW) pt 3, div 1.
23. Made under the *Privacy and Personal Information Protection Act 1998* (NSW) s 41.
24. As defined in s 6 of the *Health Records and Information Privacy Act 2002* (NSW).
25. HPP 1-4.
26. HPP 5.
27. HPP 10-11.
28. HPP 9.
29. HPP 6-8.
30. HPP 12.
31. HPP 13.
32. HPP 14.

health information.[33] The circumstances in which compliance is not required are listed under each HPP.

4.14 Part 1 of the Act contains the definitions, while Part 2 describes the general operation of HRIPA, including specific exemptions for particular practices and agencies. HRIPA makes special provision for the application of the HPPs to the public sector in Part 3, and to the private sector in Part 4. Privacy codes of practice and procedures for complaints against private sector persons[34] and organisations are provided for in Parts 5 and 6, respectively. Part 7 details the functions of the Privacy Commissioner, while miscellaneous provisions are located in Part 8.

Difficulties with the structure of PPIPA

4.15 A number of commentators have remarked on the labyrinthine structure of PPIPA. Indeed, the President of the New South Wales Administrative Decisions Tribunal observed that he had seen "nothing quite like the maze that the New South Wales Act presents".[35] One problem seems to be the lack of clarity that occurs due to the location of the IPPs within PPIPA. Unlike other comparable legislation, the IPPs are not sequentially numbered and located in a discrete part of the legislation, but included in the body of the Act and given section numbers. For example, rather than being referred to as IPP 1, the principle dealing with collection of personal information for lawful purposes is contained in s 8 of PPIPA.

4.16 Another matter of particular concern is the seemingly haphazard location of provisions that exempt agencies, or types of activities, from some or all of the operation of PPIPA. The exemption provisions are currently dispersed throughout the Act and may be contained in codes or regulations. This creates confusion for public sector agencies in terms of understanding their obligations under the legislation, and for members of the public who may be uncertain as to the extent to which their personal information is protected.[36]

---

33. HPP 15.
34. Note that the *Health Records and Information Privacy Act 2002* (NSW) provides for complaints against public sector agencies to be dealt with under the procedures outlined in the *Privacy and Personal Information Protection Act 1998* (NSW): see *Health Records and Information Privacy Act 2002* (NSW) s 21.
35. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (26 May 2004), 5.
36. See, for example, New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly), [5.2].

4.17 The number of exemptions from the scope and coverage of PPIPA prompted the Australian Privacy Foundation to comment that "the law creates an illusion of privacy protection in some areas which is not delivered".[37] A recent statutory review of PPIPA undertaken by the New South Wales Attorney General's Department noted that most commentators believe other examples of privacy legislation to be schematically clearer than PPIPA.[38] Accordingly, the review recommended that PPIPA be restructured using HRIPA as a model.[39] The review further recommended that the IPPs, together with the exemptions relevant to each, be located in a schedule to the Act, as in HRIPA.[40] Privacy NSW has also expressed the view that PPIPA should be restructured to bring all Act-based exemptions and exceptions together in one Part or Schedule.[41]

Level of detail

4.18 As noted above, both PPIPA and HRIPA are essentially examples of principles-based legislation, in that they each have as their core a set of privacy principles that articulate desired outcomes for information protection. However, the principles do more than state outcomes. In particular, PPIPA and its IPPs are reasonably prescriptive.

4.19 Privacy NSW is of the opinion that PPIPA is an example of "principle-based legislation being applied in a legal system which is

37. See Australian Privacy Foundation, *Submission to the New South Wales Attorney General's Department's Review of the Privacy and Personal Information Protection Act 1998* (2004), 2. For a discussion on the content of the exemption provisions, see Ch 3.
38. See, for example, New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [5.2]. In particular, see New South Wales Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (26 May 2004), 6; and Australian Privacy Foundation, *Submission to the New South Wales Attorney General's Department's Review of the Privacy and Personal Information Protection Act 1998*, 2.
39. See, for example, New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, Recommendation 2.
40. See, for example, New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, Recommendation 2 and [5.6]. The New South Wales Government supports that recommendation, but awaits the outcome of the reviews of privacy legislation being conducted by this Commission and the ALRC: see New South Wales Government, *Response to the Report on the Statutory Review of the Privacy and Personal Information Protection Act 1998*, 3.
41. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998* (24 June 2004), 43.

more familiar with applying legal rules".[42] It considers that the principles on which PPIPA is based are sound. However, the legislative mechanisms designed to achieve compliance can be too rigid. This has led to the insertion of wholesale exemptions for specific functions or for certain agencies.[43] Privacy NSW believes HRIPA to be a better model in this regard, stating higher-level principles, with provision for the Privacy Commissioner to make statutory guidelines on detailed matters of compliance not suited to inclusion in legislation.[44] Accordingly, Privacy NSW is of the view that PPIPA should be amended to distinguish more clearly between the core principles in the legislation, and the mechanisms by which those principles could be expected to be achieved.[45]

4.20 This view accords with that of the ALRC. In DP 72, the ALRC favoured the development of a set of Unified Privacy Principles (or "UPPs") to be contained in the *Privacy Act 1988* (Cth), which would apply across the public and private sectors. The ALRC argues that the move towards a single set of privacy principles would be more easily facilitated through legislation that is not overly prescriptive. Accordingly, the ALRC proposes that the UPPs should be drafted as high-level principles that are simple, clear and easy to understand and apply.[46] Further, the ALRC proposes that those principles should be able to be modified by more detailed agency and sector-specific rules to be contained in the regulations.[47]

The Commission's view

4.21 The regulation of the way in which personal information is handled by the New South Wales public sector, from collection through to disclosure, is a complex matter involving a diversity of contexts. As such, legislation that underpins that regulation must involve a degree of complexity. However, the Commission is of the view that PPIPA in particular is unnecessarily convoluted. It is extremely difficult to identify which agencies are covered by all or some of the IPPs, and which agencies and activities have complete or partial exemption from the coverage of PPIPA as a whole. Indeed, the

---

42. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, 40.
43. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, 8-9.
44. See *Health Records and Information Privacy Act 2002* (NSW) s 64.
45. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, 42.
46. ALRC DP 72, Proposal 15-1.
47. ALRC DP 72, Proposals 15-1 and 3-1.

number of exceptions and exemptions is such that, even when presented in tabular form, they run to several pages.[48]

4.22 Segregating the IPPs into a Schedule to the Act, followed by exceptions to each IPP, would increase the transparency of PPIPA. This would also bring PPIPA into line with other information privacy laws, such as HRIPA, the *Information Privacy Act 2000* (Vic), and the *Privacy Act 1988* (Cth). This would also accord with the ALRC's proposal to consolidate the two sets of principles in the *Privacy Act 1988* (Cth) into a single set of UPPs, and to clarify and group together the exemptions into a separate part of the Act.[49]

4.23 Similarly, there is an attraction in the proposal to pare down the IPPs to high level principles, leaving the detail of how to comply with the principles, and any agency or sector-specific provisions, to be dealt with in the regulations. This has the advantage of making the legislation clearer and as flexible as possible. Consistency of compliance may be aided by making the legislation as prescriptive as possible; however, the current state of confusion that seems to surround privacy laws, and PPIPA in particular, suggests that it is the complexity of the provisions that is undermining their effectiveness.

4.24 As noted by the ALRC in DP 72, the broad, national application of the proposed UPPs would be facilitated by being framed as high-level principles. We agree. We propose:

- restructuring PPIPA to locate the IPPs and exemptions in a Schedule to the Act, and
- reducing PPIPA's level of detail and complexity to more closely resemble that of HRIPA.

---

48. See exemptions matrix at: www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/privacyessentials_04_2005.pdf/$file/privacyessentials_04_2005.pd». See also Chapter 5.
49. ALRC DP 72, Proposal 3-2.

PROPOSAL 4

The *Privacy and Personal Information Protection Act 1998* (NSW) should be restructured:

- to locate the IPPs and exemptions in a schedule to the Act; and
- to reduce the Act's level of detail and complexity to resemble more closely the structure of the Health Records and Information Privacy Act 2002 (NSW).

SHOULD PPIPA HAVE AN OBJECTS CLAUSE?

4.25 It has become fairly common practice for legislation to contain either an objects clause, or a statement of purpose, or both. An objects clause or a statement of purpose can operate as a "coathanger" on which the structure of the legislation hangs. It can also be a useful tool of statutory interpretation should questions of uncertainty or ambiguity arise.[50] An objects clause may contain a broad statement of social aims to be derived from the legislation, whereas a statement of purpose may have a narrower focus of clarifying the legislative intent. In terms of privacy legislation, PPIPA is quite unusual in that it has neither, while HRIPA contains both.[51]

4.26 At the Commonwealth level, the *Privacy Amendment (Private Sector) Act 2000* (Cth) contains an objects clause,[52] but the *Privacy Act 1988* (Cth) does not. In IP 31, the ALRC noted the absence of an objects clause in the latter Act, and asked if there were some benefit to be derived from the inclusion of such a clause.[53] After receiving feedback on what should be included in an objects clause, the ALRC proposed in DP 72, that the *Privacy Act 1988* (Cth) should contain the following statement of objects:

> (a) implement Australia's obligations at international law in relation to privacy;
>
> (b) promote the protection of individual privacy;
>
> (c) recognise that the right to privacy is not absolute and to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests;
>
> (d) establish a cause of action to protect the interests that individuals have in the personal sphere free from interference from others;

---

50. See *Interpretation Act 1987* (NSW) s 33.
51. *Health Records and Information Privacy Act 2002* (NSW) s 3(1) and s 3(2). There is also an objects clause in the *Health Records Act 2001* (Vic) s 6; and the *Information Act 2002* (NT) s 3(1).
52. *Privacy Amendment (Private Sector) Act 2000* (Cth) s 3.
53. ALRC IP 31, [3.15]-[3.21].

(e) promote the responsible and transparent handling of personal information by agencies and organisations;

(f) facilitate the growth and development of electronic commerce, nationally and internationally, while ensuring respect for the right to privacy; and

(g) provide the basis for nationally consistent regulation of privacy.[54]

The Commission's view

4.27 The Commission holds the preliminary view that an objects clause and/or a statement of purpose would be a beneficial inclusion in PPIPA. It would act as an interpretative aid, and provide a structural focal point for the Act. The objects clause proposed by the ALRC serves as a helpful illustration of the types of matters that could be included in PPIPA. However, not all of those objects would be appropriate for State legislation that applies only to the public sector.

4.28 Perhaps the best example of an objects clause and a statement of purpose in privacy legislation directly comparable to PPIPA is that contained in the *Information Privacy Act 2000* (Vic). The main purposes of the *Information Privacy Act 2000* (Vic) are stated to be:

(a) to establish a regime for the responsible collection and handling of personal information in the Victorian public sector;

(b) to provide individuals with rights of access to information about them held by organisations, including information held by contracted service providers;

(c) to provide individuals with the right to require an organisation to correct information about them held by the organisation, including information held by contracted service providers;

(d) to provide remedies for interferences with the information privacy of an individual;

(e) to provide for the appointment of a Privacy Commissioner.[55]

4.29 In addition, the Victorian *Information Privacy Act 2000* contains the following statement of objects:

(a) to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;

(b) to promote awareness of responsible personal information handling practices in the public sector;

---

54. ALRC DP 72, Proposal 3-4.
55. *Information Privacy Act 2000* (Vic) s 1.

(c) to promote the responsible and transparent handling of personal information in the public sector.[56]

These objects also accord largely with those articulated in the Second Reading Speech that introduced PPIPA into New South Wales Parliament.[57]

4.30 We seek comment on whether or not PPIPA should contain an objects clause and/or statement of purpose, and, if so, how such a clause or statement should be framed.

ISSUE 3

Should the *Privacy and Personal Information Protection Act 1998* (NSW) contain an objects clause? If so, how should that clause be drafted?

ACHIEVING GREATER CONSISTENCY IN HEALTH INFORMATION

4.31 One issue that has generated significant debate in recent years is the regulation of health information privacy, and the problems caused by the lack of any nationally consistent approach. Consistency in this context has at least three dimensions, namely, consistency between: Commonwealth and State laws; legislation that applies to the public and private health care sectors; and laws that regulate the privacy of general, as well as health-specific, information. The latter is particularly important, given that a number of agencies and organisations hold both general and health information and must currently comply with different privacy principles for each.

4.32 At the Commonwealth level, health information is regulated under the general IPPs and NPPs (or National Privacy Principles) in the *Privacy Act 1988* (Cth) that apply to the public and private sectors respectively. Other jurisdictions, such as New South Wales and Victoria, have health specific information privacy laws that apply to both the public and private sectors. This can lead health care providers in border regions, such as Albury-Wodonga, having to comply with as many as 36 similar, but not necessarily consistent, privacy principles under three different pieces of legislation.[58]

---

56. *Information Privacy Act 2000* (Vic) s 5.
57. See New South Wales, *Parliamentary Debates*, Legislative Council, 17 September 1998, 7598-99 (the Hon J W Shaw). See Ch 3 for more details of the objects of the *Privacy and Personal Information Protection Act 1998* (NSW).
58. That is, the 10 NPPs in the *Privacy Act 1988* (Cth), the 15 in the *Health Records and Information Privacy Act 2002* (NSW), and the 11 in the *Health Records Act 2001* (Vic).

4.33 The National Health and Medical Research Council has documented the difficulties caused by the complex plethora of health privacy laws in a health care environment where public/private and Commonwealth/State distinctions are increasingly meaningless. The Council observes that confusion among health care providers over which regime applies is common. This can lead to clinical care and quality assurance being limited because of impaired access to health information, and significant research not being approved.[59] The Council urged the Commonwealth to consider implementing a single, simplified, national health privacy regime to replace the existing regulation.[60]

4.34 The need for nationally consistent regulation of health information will be even more crucial with the advent of electronically linked information systems. Instead of separate patient files being held by public or private hospitals, general practitioners and medical specialists, there is a move towards national electronic files where patient health records could be shared by health care professionals. For example, the Commonwealth's Health*Connect* initiative proposes that electronic referrals could be sent from one health care provider to another, and patient information shared electronically between hospitals and aged care facilities.[61] In NSW, a system called *Healthelink*, is currently being piloted in the Maitland region and in Greater Western Sydney for particular demographic groups.[62]

4.35 These measures will undoubtedly result in benefits in terms of service delivery and more streamlined procedures for both patients and health care practitioners. However, the privacy implications of health information being electronically stored, linked and shared, present enormous challenges. A number of initiatives, such as the draft National Health Privacy Code and the establishment of the National E-Health Transition Authority,[63] have been underway for some time in order to help address these challenges.

---

59. National Health and Medical Research Council, *Submission to the Review by the Federal Privacy Commissioner of the Private Sector Provisions of the Privacy Act 1988* (Cth) (10 December 2004), [4.1-4.2].
60. National Health and Medical Research Council, *Submission to the Review by the Federal Privacy Commissioner of the Private Sector Provisions of the Privacy Act 1988* (Cth), Recommendation 1.
61. For more information, see «www.healthconnect.gov.au».
62. See «www.healthelink.nsw.gov.au» accessed at 22 May 2008.
63. The National E-Health Transition Authority is a not-for profit company jointly funded and established by the Commonwealth and State and Territory Governments to "develop better ways of electronically collecting and securely exchanging health information": see «www.nehta.gov.au», accessed at 14 November 2007.

4.36 The case for national consistency in the regulation of health information privacy is difficult to oppose.[64] These matters are currently being consulted on extensively by the ALRC, and we will carefully consider the public feedback to their inquiry. In this section, we examine the impact on the structure of New South Wales privacy laws of the ALRC's proposals aimed at achieving national consistency. In particular, we ask whether HRIPA should be restructured in terms of its private sector coverage and, if so, what implications this would hold for the regulation of health information held by public sector agencies.

Private sector coverage of health information under HRIPA

4.37 While national consistency in information privacy regulation as a whole is a worthy goal, it is the coverage of private sector organisations that represents the biggest area of overlap, inconsistency and controversy. Adherence to numerous provisions across different jurisdictions leads to added compliance burdens for business. Consumers and organisations may be confused as to their rights and responsibilities with regard to personal information. These concerns are particularly acute for private sector organisations that deal with health information, since this is the only area that is regulated by both Commonwealth and State privacy legislation.[65]

4.38 There have been a number of calls for the Commonwealth and States to synthesise their laws regarding health privacy.[66] In 2003, the ALRC recommended, in its Report on the protection of human genetic information, that the Commonwealth and the States and Territories should attempt to harmonise information and health privacy legislation.[67] In 2005, the Federal Privacy Commissioner noted the confusion caused by the proliferation of State health privacy laws. She recommended that the Commonwealth Government should remove any further ambiguity by amending s 3 of the *Privacy Act 1988* (Cth) to provide that the Commonwealth intended to "cover the field" so far as regulation of information privacy in the private sector is concerned.[68]

---

64 See Ch 1 at para 1.7-1.9 and Proposal 1.1.

65. At least in New South Wales, Victoria and the ACT.

66. See New South Wales Health, *Submission* (18 September 2006); and the Royal Australian College of General Practitioners New South Wales and ACT Faculty, *Submission* (7 July 2006).

67. Australian Law Reform Commission, *Essentially Yours*, (Report 96, 2003) vol 1, 251, Recommendation 7.1.

68. Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988 (2005)*, 45.

4.39 The ALRC has taken up this recommendation in DP 72, proposing that the *Privacy Act 1988* (Cth) be amended to preclude State and Territory laws that regulate the handling of personal information in the private sector.[69] As far as New South Wales is concerned, this would have the effect of invalidating HRIPA to the extent that it applies to the private sector's dealings with health information. The privacy of all information, including health information, dealt with by the private sector would be regulated federally under the UPPs.

The Commission's view

4.40 If the ALRC's proposals were to be implemented, New South Wales would have to amend HRIPA so that it no longer applied to private sector organisations.[70] This would be highly beneficial for multi-disciplinary organisations, or those that operate across State jurisdictions, since they would only need to comply with one set of privacy principles. It would also make it easier for consumers to know which law regulates access to, and protection of, their health information.

4.41 NSW would - and should -continue to have a role in regulating health information held by State public sector agencies and private sector contractors that deal with those agencies.[71] This is vital given the New South Wales Government's role in the management and delivery of health care services in this State. Also, the ALRC acknowledges the importance of complaints handling at a local level, and proposes that State and Territory complaint agencies should be delegated the power to deal with complaints concerning alleged interferences with health information privacy by private sector organisations.[72]

4.42 At this preliminary stage, we support the ALRC's proposal in this regard, given the benefits that would flow. Before making any final recommendation, however, we would like to obtain the views of consumers and businesses who would be affected by the proposal for New South Wales to hand over to the Commonwealth responsibility for health information protection in the private sector.

---

69. ALRC DP 72, Proposal 4-1.
70. See ALRC DP 72, Proposal 4-2. The ALRC notes that provisions exist in other State legislation, such as the *Public Health Act 1991* (NSW) s 14, that require reporting of certain information for public health purposes, and believes that there are good reasons why these provisions should be preserved: see ALRC DP 72, [4.75]-[4.76].
71. See ALRC DP 72, Proposal 4-3.
72. ALRC DP 72, Proposals 45-3 and 56-1.

PROPOSAL 5

The *Health Records and Information Privacy Act 2002* (NSW) should be amended so that the handling of health information by private sector organisations is regulated under the *Privacy Act 1988* (Cth).

Should health information continue to be regulated separately?

4.43 When HRIPA was enacted in 2002, the privacy of health information was considered to raise issues of sufficient specificity to warrant separate legislative treatment. The Second Reading Speech made mention of the need to accommodate the "special needs arising in the management and use of health information", and the need to balance consumer privacy with effective delivery of health care services.[73] This followed a Ministerial Advisory Committee Report that recommended that separate health-specific legislation be introduced. The recommendation was largely based on the need for seamless regulation of information held by both the private and the public sectors, and because of the challenges posed by the foreshadowed national electronic linking of health records.[74] There was a concern among the authors of the report that the legislative framework governing privacy at that time was inadequate to deal with what were seen as needs peculiar to health information.[75]

4.44 Victoria has also opted for health-specific information privacy legislation. When introducing the *Health Records Act 2001* (Vic), the Minister for Health described health information as "arguably the most sensitive category of personal information that exists about an individual". He also noted that the legislation recognised and responded to the "threat to privacy posed by the exponentially increasing capacity of modern technology" which was "nowhere more evident than in the case of health information".[76]

4.45 On the other hand, health information is not subject to separate regulation at the Commonwealth level. The question of whether or not health information should be included under the general provisions of the *Privacy Act 1988* (Cth) was hotly debated during the passage of

73. See New South Wales, *Parliamentary Debates*, Legislative Council, 11 June 2002, 2958 (Michael Egan).
74. New South Wales Ministerial Advisory Committee on Privacy and Health Information, *Panacea or Placebo?*, *Report to the New South Wales Minister for Health* (2000).
75. New South Wales Ministerial Advisory Committee on Privacy and Health Information, *Panacea or Placebo? Report to the New South Wales Minister for Health*, 22-24.
76. Victoria, *Parliamentary Debates*, Legislative Assembly, 23 November 2000, 1906 (John Thwaites).

the *Privacy Amendment (Private Sector) Bill 2000*.[77] The House of Representatives Standing Committee on Legal and Constitutional Affairs noted that there were three principal arguments against including health information in the Bill:

- The health sector is so different from other sectors that the attempt to incorporate it within the general framework of the Bill was misguided.
- The regime established by the Bill would lead to the creation of inconsistent standards governing privacy rights in the public and private sectors.
- The access rights contained in the Bill enabling individuals to access their own health information were totally inadequate.[78]

4.46 Despite these arguments, the Committee concluded that health information should be included in the general Bill until such time when the health care sector could reach agreement on the harmonisation of privacy principles applicable to the public and private sectors.[79]

The ALRC's position

4.47 The ALRC notes that, while the handling of health information gives rise to some unique issues, it is undesirable to have a separate set of principles or legislation dealing with health information privacy.[80] This view is based on the need to avoid inconsistency between general and health-specific privacy regimes, and the fact that health information is held in a range of contexts, many of which have nothing to do with providing health care services.[81] Many organisations hold a combination of general personal and health information, and should not, in the ALRC's view, be required to comply with two sets of principles.[82]

---

77. See Australia, House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), Ch 6.
78. Australia, House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*, [6.12].
79. Australia, House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*, [6.29]-[6.40].
80. ALRC DP 72, [56.73]-[56.74].
81. See, for example, *AW v Vice Chancellor, University of Newcastle* [2008] NSWADT 86 in which health information (the applicant's HIV status) was held by the university in the context of the applicant's complaint to the university of discrimination and harassment (the information having been provided by the applicant to support his allegations).
82. ALRC DP 72, [56.77]-[56.78].

4.48 Accordingly, the ALRC proposes that health information held by the public and private sectors should be regulated by the proposed UPPs. Further, the ALRC proposes that any amendments to the UPPs that may be necessary due to the unique nature of health information should be included in regulations made under the *Privacy Act 1988* (Cth).[83] Those regulations could be based on the draft National Health Privacy Code.[84]

The Commission's view

4.49 If the proposal to hand over the regulation of private sector health information privacy were to be adopted, this would leave New South Wales with two main privacy statutes. Both would cover public sector entities only, but one would contain health-specific provisions.

4.50 At this stage, should that proposal be adopted, we favour merging PPIPA and HRIPA into a single piece of privacy legislation.[85] We acknowledge that health information privacy does raise some issues of particular concern, but agree with the ALRC that those concerns can be accommodated through regulations or national codes, rather than through separate legislation. However, we have not reached a definite conclusion on the matter, and invite submissions on the topic.

ISSUE 4

If health information held by the private sector were to be regulated by the *Privacy Act 1988* (Cth), should New South Wales continue to have two separate information privacy statutes?

ISSUE 5

What reasons would there be for the continued existence of the *Health Records and Information Privacy Act 2002* (NSW) if it only regulated public sector agencies?

83. ALRC DP 72, Proposal 56-2.
84. ALRC DP 72, [56.83].
85. We propose that that legislation should be modelled on the *Health Records and Information Privacy Act 2002* (NSW) structure.

5. Scope of privacy protection

- Introduction
- Should the scope of PPIPA and HRIPA be expanded by reducing or limiting exemptions?
- Should other aspects of privacy be expressly protected in PPIPA?
- A general cause of action for invasion of privacy?

INTRODUCTION

5.1 Chapter 3 described the protection of privacy that the *Privacy and Personal Information Protection Act 1998* (NSW) ("PPIPA") and the *Health Records and Information Privacy Act 2002* (NSW) ("HRIPA") afford to individuals whose information is collected, held, used and disclosed by public sector agencies and private sector persons.

5.2 This chapter considers whether the scope of PPIPA and/or HRIPA can or should be extended:

- by limiting the numerous exemptions in the legislation, particularly exemptions to the definition of "personal information"; and/or
- by giving express protection to areas, subject matters or activities beyond information privacy.

5.3 In regard to the latter option, although PPIPA already extends beyond the protection of information privacy, it does so indeterminately. This chapter inquires into whether PPIPA's protection of general invasions of privacy, including physical privacy, should be express and definitive, putting boundaries of its reach in place. It also considers whether an expanded range of remedies should be made available under PPIPA for breaches of privacy. Impacting on this inquiry is the prospect of a statutory cause of action for invasion of privacy, giving rise to the challenge of how to reconcile the application and jurisdiction of all privacy laws that may then operate in New South Wales.

SHOULD THE SCOPE OF PPIPA AND HRIPA BE EXPANDED BY REDUCING OR LIMITING EXEMPTIONS?

Background

5.4 The scope of the legislation, and the application of PPIPA's Information Protection Principles ("IPPs") and HRIPA's Health Privacy Principles ("HPPs"), is curtailed by the number of exemptions - from the definition of "personal information"; of specific functions; or of specific agencies.[1] As Chapter 4 put forward, there are arguably too

1. Exemptions can also be created in regulations, codes of practice and public interest directions but this discussion is confined to exemptions under the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) themselves.

many exemptions, both in terms of restricting the extent of protection given to the public and in terms of the public's ability to make sense of the legislation. The complexity of the legislation created by the number of exceptions also engenders challenges to the way the legislation is applied, which consume time, money and energy. Individual's are forced to seek internal review of conduct or a decision that has exempted their personal information from the safeguards of the IPPs, with binding findings and enforceable remedies only available on subsequent application to the Administrative Decisions Tribunal ("ADT").

5.5 The paragraphs below single out some of the exemptions that have been the subject of criticism and examine whether any of these can be omitted or limited. Most fall into the category of exemptions to the definition of "personal information".

5.6 The issues raised by the Commission should be considered in the context of PPIPA and HRIPA being beneficial statutes that, subject to the identified purposes of the statutes, "should be interpreted broadly so that people can obtain the maximum benefit from the rights they are afforded".[2] In general, legislation affecting privacy rights should be interpreted so as to allow minimal exceptions to the general rules that protect an individual's privacy.[3]

Personal information – PPIPA s 4; HRIPA s 5

5.7 Both s 4 of PPIPA and s 5 of HRIPA define "personal information" as meaning "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". Standing alone, this is a relatively straightforward and broad definition. However, each section then goes on to provide, in sub-section (3), that "personal information does not include the following", thereafter listing 12 exceptions to the definition in the case of PPIPA and 15 exceptions in the case of HRIPA.[4]

---

2. *GA v Department of Education and Training and New South Wales Police* (GD) [2004] NSWADTAP 18, [48] (in relation to PPIPA).
3. *Coco v The Queen* (1994) 179 CLR 427; *Taciak v Commissioner of Australian Federal Police* (1995) 131 ALR 319.
4. The exceptions contained in s 4(3)(a)-(j) and (k) of PPIPA are mirrored in s 5(3)(a), (b), (f)-(m) and (o) of HRIPA. HRIPA does not except adoption information obtained under the *Adoption Act 2000* (NSW), as PPIPA does in s 4(3)(ja). HRIPA has four further exceptions that PPIPA does not have: s 5(3)(c) - information contained in a document kept in a library, art gallery

5.8 The ADT has commented (in reference to PPIPA) that the broad definition of "personal information" is cut back in "quite significant and detrimental ways".[5] The NSW Ombudsman has also observed that PPIPA's 12 separate exceptions "result in an overly complicated definition which is a barrier to effective understanding and implementation of the Act".[6]

5.9 Privacy NSW has argued that it would be preferable to provide exemptions from specific IPPs, rather than taking certain categories of personal information outside the scope of the legislation altogether.[7] This is an approach that could equally be adopted in relation to specific functions and agencies exempted by PPIPA and HRIPA. Rather than blanket exemption from the IPPs and HPPs, the legislation could identify just those IPPs and HPPs whose application may genuinely interfere with an agency's legitimate functioning and purposes.

5.10 Privacy NSW has also pointed out that many exemptions from the definition of "personal information", particularly those applying to information about protected witnesses, adoption information and information obtained through telephone interceptions, "relate to matters that would otherwise be subject to tough sanctions for corrupt disclosure".[8]

Publicly available information - PPIPA s 4(3)(b); generally available information - HRIPA s 5(3)(b)

5.11 PPIPA provides that information about an individual that is contained in a *publicly available* publication is excepted from the

---

or museum for purposes of reference study or exhibition; (d) – information contained in a record available for public inspection under the *State Records Act 1998* (NSW); (e) – information contained in archives within the meaning of the *Copyright Act 1968* (Cth) and (n) – information forming part of an employee record within the meaning of the *Privacy Act 1988* (Cth) held by a private sector person.

5. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (26 May 2004), 5.
6. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (April 2004), 28.
7. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998* (2004), [3.1.2], 63. See also New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, (Tabled 25 September 2007, Legislative Assembly), [9.9].
8. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998* (2004), [3.1.2], 63. See also New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.9].

definition of "personal information". HRIPA provides that information about an individual that is contained in a *generally available* publication is excepted from the definition of "personal information". Neither Act specifically defines these phrases. PPIPA provides that a regulation can declare a publication or document not to be a "publicly available document" for the purposes of that Act.[9] The effect of s 4(3)(b) of PPIPA and s 5(3)(b) of HRIPA is that public sector agencies can collect and use information from published sources without having to comply with restrictions imposed by the IPPs, although the annotated guide to PPIPA states that "there must be some provable nexus between the information in the publication and the issue at the time of the conduct."[10]

5.12 Privacy NSW has argued that the absence of a clear definition in PPIPA of "publicly available publication" has caused confusion and disagreement about the application and scope of the exception.[11] It is concerned that the exception is both unclear and too wide, effectively undermining the object of PPIPA.[12] Furthermore, it "places much of people's information at risk of misuse without penalty".[13] Privacy NSW submits that the drafting of s 4(3) allows information collected from a publicly available publication "to be used or disclosed in ways that would be considered corrupt and be subject to the criminal offence provisions of the Act, were it not for the exemption".[14] Combined with the exemption in s 28(3) for disclosures to an agency's minister or the Premier, Privacy NSW has submitted that s 4(3)(b) "allows 'information laundering' to occur".[15]

5.13 Submissions to the Attorney General's Department's statutory review of PPIPA were concerned that "publicly available information"

---

9. *Privacy and Personal Information Protection Act 1998* (NSW) s 3.
10. A Johnston, *PPIPA in Practice: An Annotated Guide to the Privacy and Personal Information Protection Act 1998* (*NSW*) (2007), [22].
11. Privacy NSW illustrates this unsatisfactory lack of clarity by asking "What is a publication?" and "How widely must it be distributed or read for it to be considered 'publicly available'?": Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, [3.1.2], 64. The existence of a distinct exemption relating to information on a "public register" creates further uncertainty.
12. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, [3.1.2], 64.
13. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, [3.1.2], 64. See also New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.17].
14. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, [3.1.2], 63.
15. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, [3.1.2], 64.

means "information in the public domain", which would include information published on the Internet.[16] If that information is inaccurate, or taken out of context, the person to whom the information relates loses important privacy protections. For example, an address published on the Internet may be obscurely placed and/or published with the expectation of very limited readership (such as a family biography/reunion site). If it is "collected" by an agency it could be highlighted and given a different context.

5.14 This risk arises in relation to all publicly available information. If it is put to a use that places the information in a different context it may give rise to inferences that did not otherwise arise, or emphasise or bring attention to it in a way that would not otherwise have occurred. The ADT Appeal Panel gives the example of the information conveyed by a name and address in a telephone directory compared with the information conveyed if that name and address is held in the file of a child protection agency.[17] Privacy NSW notes that in 2002-2003, 22% of all internal review cases involved alleged misuse of personal contact details.[18] The exemption had in many cases been used to justify disclosure of a complainant's identity to a third party on the basis that the information was published in a telephone directory. Privacy NSW gives a further example of the former Special Branch of the NSW Police creating dossiers on individuals from publicly available sources such as press clippings.

5.15 Taking out of a person's control the choice of when, where and to whom he or she discloses personal information has serious privacy implications and calls for proper justification and strict safeguards. As Privacy NSW has said, "context is everything".[19]

5.16 The ADT Appeal Panel has signalled that particularly convincing or compelling evidence will be required before it finds that something is from a publicly available publication, resulting in the individual named being unable to "access the important human rights protections conferred by [PPIPA]".[20]

16. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.18].
17. *Commissioner of Police, New South Wales v EG; EG v Commissioner of Police, New South Wales* (GD) [2004] NSWADTAP 10.
18. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, [3.1.2], 64.
19. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998*, [3.1.2], 65.
20. *NW v Fire Brigades* [2005] NSWADT 73, [32]. See A Johnston, *PPIPA in Practice: An Annotated Guide to the Privacy and Personal Information Protection Act 1998 (NSW)*, [21].

5.17 The statutory review of PPIPA concluded that:

> 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.[21]

5.18 If the ADT is reluctant to find that information is "publicly available", and the fair application of the exemption is dependent on the reasonableness of the relevant agency, it has to be asked whether it is either justified or sound to maintain this exemption to the definition of "personal information".

5.19 The Privacy Commissioner has suggested that it would be preferable to remove the general exemption and instead exempt publicly available information only from IPP 2, which provides that information can only be collected from the person concerned, unless that person has consented to third party collection.[22] The Commission sees merit in that proposal and is interested to receive submissions on it.

5.20 The ADT has also expressed a concern that the exception is too wide.[23] For example, agencies have indicated to the ADT that documents used for internal management purposes but not restricted and therefore, strictly speaking, "publicly available", are covered by the exception.[24] In the ADT's view, "publicly available information" should not be exempted generally, but only from the collection IPPs, as in the *Privacy Act 1988* (Cth).[25]

5.21 Whether the above analysis and submissions in relation to "publicly available" information are equally applicable to "generally available" information is uncertain. It can be argued that the meaning of "generally available" is narrower than the meaning of "publicly

---

21. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998* (2004), [3.1.2], 66. See also New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.20].
22. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.17].
23. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 10.
24. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 10.
25. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 10.

available", as one might expect where the information relates to an individual's health. Whether the terms ought to be distinguished in this way is a further issue. The Commission would like to receive submissions on the point.

Interaction of s 4(3)(e), (i) and (ja) with s 20(5) of PPIPA; interaction of s 5(3)(h) and (l) with s 22(3) of HRIPA

5.22 Sections 4(3)(e) and (i) of PPIPA are mirrored in s 5(3)(h) and (l) of HRIPA, and s 20(5) of PPIPA is mirrored in s 22(3) of HRIPA. For ease of reading, the following discussion focuses on PPIPA but the comments are equally applicable to the provisions of HRIPA. There is, however, no equivalent provision in HRIPA of s 4(3)(ja) of PPIPA (adoption information).

5.23 ***Protected disclosures – PPIPA s 4 (3)(e); HRIPA s 5(3)(h).*** Section 4(3)(e) excludes from the definition of "personal information" information contained in a "protected disclosure" within the meaning of the *Protected Disclosures Act 1994* (NSW), or collected in the course of an investigation arising out of a protected disclosure. A "protected disclosure" is one made by a public official to an investigating authority,[26] for the purpose of uncovering corrupt conduct, maladministration or serious and substantial waste in the public sector.[27]

5.24 The NSW Ombudsman argues that the exemption is unnecessary because of the provisions of s 20(5) of PPIPA and cl 20(1)(d) of Schedule 1 to the *Freedom of Information Act 1989* (NSW) ("FOI Act"). Clause 20(1)(d) of Schedule 1 to the FOI Act exempts documents from the operation of that Act that contain matter relating to a protected disclosure. The effect of s 20(5) in this context is (presumably) to ensure that provisions of the FOI Act that exempt information from the application of IPPs 6, 7 and 8 (s 13, 14 and 15) apply, unaffected by PPIPA.[28]

5.25 However, this interpretation of s 20(5) is based on an assumption that the exemption in cl 20(1)(d) of Schedule 1 to the FOI Act can be classified as a "condition" or "limitation" so as to come within the ambit of s 20(5).[29] This assumption may not be correct. The

---

26. *Protected Disclosures Act 1994* (NSW) s 8.
27. *Protected Disclosure Act 1994* (NSW) s 3.
28. IPP 6 allows a person to discover whether the agency holds personal information; and IPPs 7 and 8 give an individual rights to access, and require amendments to, his or her personal information.
29. Section 20(5) of PPIPA provides: "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

Crown Solicitor's Office, New South Wales ("Crown Solicitor"), commenting that s 20(5) is "not an easy provision to construe", has observed that "[t]he difficulty lies in identifying the provisions of the FOI Act that impose 'conditions or limitations (however expressed)' with respect to any 'matter' referred to in ss 13, 14 or 15".[30]

5.26 Given that the wording of s 20(5) of PPIPA is not easy to decipher, and arguably ambiguous,[31] it may be imprudent to do away with the exemption in s 4(3)(e) in reliance on such an unclear provision. The protected disclosure exemption is a valid one as there is legitimate public interest in allowing a public official to disclose information to an investigating authority in the knowledge that that information will be exempt not only from IPPs 6, 7 and 8 but from other relevant IPPs.

5.27 However, whether the disclosure should be exempt from all the IPPs needs individual consideration. For example, it is perhaps not justified to exempt the disclosure from IPP 1, which provides that an agency must not collect personal information other than for a lawful purpose by lawful means. Similarly, should the disclosure be exempt from: IPP 5 (retention of information for no longer than is necessary; secure keeping and disposal); IPP 9 (checking accuracy of information before use); or IPP 10 (use of information for the purpose for which it was collected, or a directly related purpose)?

5.28 ***Restricted documents – PPIPA s 4(3)(i); HRIPA s 5(3)(l).*** The NSW Ombudsman raises a similar argument with respect to the exception in s 4(3)(i), again submitting that it is unnecessary because of s 20(5) of PPIPA.[32] Section 4(3)(i) excepts information contained in "restricted documents", namely Cabinet and Executive Council documents, as referred to in cl 1 and 2 respectively of Schedule 1 to the FOI Act.

5.29 ***Adoption information – PPIPA s 4(3)(ja).*** Section 4(3)(ja) excepts adoption information obtained under the *Adoption Act 2000* (NSW) from the definition of "personal information". Clause 20(1)(c) of Schedule 1 to the FOI Act exempts from the operation of that Act "matter relating to the receipt of an amended or original birth certificate or of prescribed information under the *Adoption Act 2000*". The NSW Ombudsman argues that s 4(3)(ja) is unnecessary by reason of s 20(5) of PPIPA and cl 20(1)(c) of Schedule 1 to the FOI Act,

---

those provisions continue to apply in relation to any such matter as if those provisions were part of this Act."

30. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [7.1].
31. See NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998*, 19.
32. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998*, 28.

providing a "suitable amendment" is made to that clause.[33] The Ombudsman does not identify what that amendment should be.

Complaints made about police – PPIPA s 4(3)(h); HRIPA s 5(3)(k)

5.30 Section 4(3)(h) of PPIPA and s 5(3)(k) of HRIPA exclude from the definition of "personal information" information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990* (NSW) (Complaints about conduct of police officers).

5.31 The ADT Appeal Panel has accepted the desirability of setting limits on the scope of the exemption, stating, in relation to PPIPA, that s 4(3)(h) would not protect information that had an "indeterminate" or "tenuous" relationship – and, even more so, no relationship at all – with the investigation.[34]

5.32 NSW Police argue that the exemption is needed, and that "arising out of" should not be interpreted so narrowly as only to exempt information that is relevant. Otherwise, the Police argue, they will be hindered in investigating and preventing police corruption because of the difficulty in determining whether a piece of information is going to be relevant or not.[35]

5.33 The review of PPIPA has observed that the phrase "arising out of" has made the exception "extremely difficult to define" and has in fact allowed its scope to be extended beyond that intended by Parliament.[36] It is critical that the provision impels a forensic exercise of tracing back the origins of the information, rather than considering the information in the context of its collection, use or disclosure. The review advocates identifying those IPPs that it is appropriate to exclude, and allowing the remainder to apply.

5.34 The NSW Ombudsman has argued that it would be unnecessary to have the exception in s 4(3)(h) of PPIPA if the Ombudsman was included in s 27.[37] Section 27 provides that the Independent Commission Against Corruption, the Police Integrity Commission, their respective Inspectors and Inspectors' staff, the NSW Police Force and the NSW Crime Commission are not required to comply with the

---

33. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998*, 28.
34. *KO v Commissioner of Police* (GD) [2004] NSWADTAP 21, [32]. See A Johnston, *PPIPA in Practice: An Annotated Guide to the Privacy and Personal Information Protection Act 1998 (NSW)*, [23].
35. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.29].
36. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [3.1.2], 67.
37. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998*, 28.

IPPs. The equivalent provision is contained in s 17 of HRIPA. This argument applies equally to s 4(3)(c), (d) and (f) of PPIPA and s 5(3)(f), (g) and (i) of HRIPA. These sub-sections except from the definition of "personal information" information about an individual arising out of: covert surveillance; a law enforcement operation; and information about a witness in a witness protection program.

Suitability for appointment or employment as public sector official - PPIPA s 4(3)(j); HRIPA s 5(3)(m)

5.35 Pursuant to s 4(3)(j) of PPIPA and s 5(3)(m) of HRIPA, information or opinion about an individual's suitability for appointment or employment as a public sector official is excepted from the definition of personal information. Privacy NSW has raised a concern that s 4(3)(j) of PPIPA is being interpreted too broadly and exceeds Parliament's intention.[38] While Privacy NSW backs up this view with statistics of complaints made by employees against public sector agencies, the Attorney General's Department, on the other hand, argues that "there is no substantive case law to indicate that the exemption is working in a way different from that which parliament intended".[39]

5.36 Parliamentary debates on the *Privacy and Personal Information Bill* cast some doubt on whether Parliament envisaged the extent to which the exemption might be applied to information beyond the recruitment process, or even whether it might apply at all following appointment to, or employment in, a position. During debate in committee on an Opposition proposal to omit s 4(3)(j) (cl 4(3)(i) of the *Privacy and Personal Information Bill*, the Hon J P Hannaford commented:

> Effectively that means people wanting to obtain personal information about themselves in relation to possible employment will not be able to obtain it.[40]

5.37 The Hon J W Shaw asked "why that information should not be available generally to prospective employers within the public sector".[41] He also commented that:

> it is not particularly easy to formulate such a code that might not prevent sensitive information being given to a prospective

---

38. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.2].
39. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.2].
40. New South Wales, *Parliamentary Debates,* Legislative Council, In Committee, 28 October 1998, 9155 (the Hon J P Hannaford,).
41. New South Wales, *Parliamentary Debates,* Legislative Council, In Committee, 28 October 1998, 9155 (the Hon J W Shaw).

> employer where that information would be highly relevant to the employability of a particular person.[42]

5.38 The Hon Dr A Chesterfield-Evans submitted that:

> if the amendment is agreed to, a department would not be able to tell another department of problems with a job applicant. It is common for an applicant to obtain a reference from the present supervisor for a job application to another department but this proposal would make that impossible.[43]

5.39 The Attorney General's Department also stated that the intention of Parliament was that the exemption would allow "free and frank discussion" during the recruitment/promotion process.[44]

5.40 However, *Y v Director General, Department of Education* has established that s 4(3)(j) does not only refer to information that was collected in the course of a selection process.[45] It can be used to exempt information relating to an employee after he or she has been appointed or employed, which gives the provision a potentially extensive application. Even within "the routine personnel context (that of recruitment, promotion, discipline and involuntary retirement)",[46] there is still the potential for significant exclusion. Furthermore, unusual cases outside this context are possible.[47] This potentially conflicts with the purposive approach that is to be applied to any interpretation of PPIPA's provisions. Given that the purpose of PPIPA is expressed in wide-ranging terms,[48] and the legislation is beneficial legislation, any exclusion should be interpreted narrowly. However, if the natural and ordinary meaning of the phrase legitimately allows an extended application of the exemption, agencies are entitled to rely on this.

5.41 In *PN v Department of Education and Training*,[49] although the complainant's complaint against the Department for failing to apply certain IPPs to her personal information was upheld, the case highlights the scope for exempting a great deal of personal

---

42. New South Wales, *Parliamentary Debates,* Legislative Council, In Committee, 28 October 1998, 9155 (the Hon J W Shaw).
43. New South Wales, *Parliamentary Debates,* Legislative Council, In Committee, 28 October 1998, 9156 (the Hon Dr A Chesterfield-Evans).
44. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.22].
45. *Y v Director General, Department of Education* [2001] NSWADT 149.
46. *Y v Director General, Department of Education* [2001] NSWADT 149, [36].
47. See *Y v Director General, Department of Education* [2001] NSWADT 149, [36]: "it would be an unusual case where the exclusion would apply outside what I have described as the routine personnel context…"
48. PPIPA is "[a]n Act to provide for the protection of personal information, and for the protection of the privacy of individuals generally; …"
49. *PN v Department of Education and Training* [2006] NSWADT 122.

information pursuant to s 4(3)(j). An agency could conceivably mount an argument for almost every piece of information, as well as opinion,[50] it collects or receives pertaining to one of its employees. In *PN v Department of Education and Training*, for example, the Department contended that all relevant information that it collected, used or disclosed was information "touching upon" the issue of PN's employment with the Department, and was thus excluded from application of the IPPs.

5.42 Even if a decision by an agency to exempt material is successfully challenged, in the meantime, the complainant has been put through, at best, inconvenience, and, at worst, harm to career, reputation and emotional well-being. *PN v Department of Education and Training* is a case in point. The complainant was successful but endured a lengthy, and costly, process of adjudication, including an internal review by the Department, a hearing by the ADT, an appeal to the ADT Appeal Panel and remittance to the ADT for further determination when the appeal was dismissed.[51]

5.43 The ambiguity of the phrase "suitability for appointment or employment" and the latitude for variations in application is implicitly acknowledged in the fact that the ADT has said that whether or not information will be exempt under s 4(3)(j) "is to be determined by consideration of both the content and the context of the information".[52]

5.44 The Commission would be interested to receive feedback on whether s 4(3)(j) of PPIPA and s 5(3)(m) should be amended either:

- to restrict, in clear terms, its application to information relating to recruitment of an employee; or
- to clarify that it can apply to information about an employee's suitability for employment in his or her current position with the relevant agency.

5.45 There is also the question of whether there is justification at all for public sector agencies having the power to collect and use information about an employee, current or prospective, that is then not protected by IPPs or HPPs. In particular, is it proper that an individual should not have an automatic right to access personal

50. The definition of "personal information" includes opinion: PPIPA s 4(1).
51. See *Department of Education and Training v PN (GD)* [2006] NSWADTAP 66. Note that the Appeal Panel granted the Department leave to appeal because "the Department's contention was clearly arguable": [7].
52. *PN v Department of Education and Training* [2006] NSWADT 122, [56]. See *Y v Director General, Department of Education* [2001] NSWADT 149; *GL v Director-General, Department of Education and Training* [2003] NSWADT 166; and *EG v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 150.

information in connection with their employment because IPP 7 or HPP 7 does not apply?[53]

Do photographs and video images constitute "personal information"?

5.46 In *SW v Forests NSW*, the ADT held that digital photographs of SW that had been copied onto a compact disc comprised personal information about SW.[54] The Tribunal relied on a statement in *Vice-Chancellor, Macquarie University v FM* that the ordinary meaning of the words "possession or control" "connotes some form of physical object upon which or within which an information or opinion is recorded".[55] However, the Crown Solicitor has raised a concern that, "while visual images could, depending on whether an individual's identity is apparent or can reasonably be identified from the image", fall within the definition of "personal information", it is conceptually difficult to apply a number of the IPPs to images, in particular the collection IPPs 2 and 3 (PPIPA s 9 and 10).[56]

5.47 Arguably, Parliament may not have intended that the definition of "personal information" would cover visual images in photographs or videos. While the wording of s 4 may appear wide enough on its face to encompass information contained in recorded images, the context of Pt 2 Division 1, in prescribing how information must be dealt with, suggests that Parliament intended that only information that "can be collected directly from, and provided by, an individual in the ordinary sense (either by some form of communication or by the giving of bodily samples)" be covered. This would not include video records or photographs taken by an agency.[57]

---

53. Section 14 of the *Privacy and Personal Information Protection Act 1998* (NSW) provides: "A public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information."
54. *SW v Forests New South Wales* [2006] NSWADT 74. See *Vice-Chancellor, Macquarie University v FM* [2005] NSWCA 192, [34]; see also *Re Pasla and Australia Postal Corporation* (1990) 20 ALD 407, 413: film held to be personal information for the purposes of the *Privacy Act 1988* (Cth).
55. *Vice-Chancellor, Macquarie University v FM* [2005] NSWCA 192, [34].
56. Crown Solicitor 's Office, New South Wales, *Submission*, [3.9]. IPP 2 (s 9) – collection of information directly from the individual; IPP 3 (s 10) – making the individual from who information is collected aware of certain things.
57. See *Vice-Chancellor, Macquarie University v FM* [2005] NSWCA 192 where it was held that information in the minds of employees was not personal information. A key reason for the Court's conclusion was the impossibility of applying most of the IPPs to that information.

Meaning of the phrase "or can reasonably be ascertained from the information or opinion"

5.48 The Crown Solicitor has noted that the meaning of "or can reasonably be ascertained from the information or opinion" in s 4(1) of PPIPA and s 5(1) of HRIPA is ambiguous.[58] On one view, it could be interpreted expansively to permit "constructive identification". That is, the identity of an individual might not be apparent from the original information but when it is combined with extrinsic information the identity becomes apparent. The problem with this construction, the Crown Solicitor argues, is that it gives rise to uncertainty as to the point at which identity of the individual ceases to become "reasonably ascertainable".[59] It may also be inconsistent with the requirement that the individual identity "can reasonably be ascertained from the information or opinion".

5.49 In *Police Force of Western Australia v Ayton*, the Court considered the phrase in the context of FOI legislation and held that the definition does not exclude the possibility that identity can be ascertained by reference to extrinsic material.[60] But the nature of the extrinsic material is central: if it is known to a significant community of people or easily accessible to ordinary members of the public, identification from a combination of sources may still be classified as having been reasonably ascertained *from* the original information in question. It could not be so classified if the extrinsic information comes from "some obscure and lengthy process of cross-referencing and deduction from other materials".[61]

5.50 The Department of Health is of the view that ascertaining someone's identity from information or opinion is so dependent on the circumstances that attempting to clarify the meaning further in legislation would not be helpful.[62] At most, it suggests formulating broad guidelines that an agency can apply to a specific context.

---

58. Crown Solicitor 's Office, New South Wales, *Submission*, [3.5].
59. Crown Solicitor 's Office, New South Wales, *Submission*, [3.5] and [4.1].
60. *Police Force of Western Australia v Ayton* [1999] WASCA 233: "I think it must be accepted that the disclosure would be disclosure about an individual whose identity is apparent from the document, notwithstanding that reference must be made to other sources to ascertain the names of those individuals." (Wheeler J), [38].
61. *Police Force of Western Australia v Ayton* [1999] WASCA 233, (Wheeler J), [38].
62. NSW Department of Health, *Consultation* (3 December 2007).

Issues arising out of the exceptions to "personal information"

ISSUE 6

(a) Should "publicly available information" under the *Privacy and Personal Information Protection Act 1998* (NSW) and "generally available information" under the *Health Records and Information Privacy Act 2002* (NSW) be exempted altogether from the definition of "personal information" in those Acts?

(b) Should IPP 2 and HPP 2 alone apply to "publicly available information" and "generally available information", but not other IPPs and HPPs?

ISSUE 7

(a) Is the meaning of "publicly available information" the same as "generally available information"? Is it appropriate that they have different meanings in the context of general information and health information?

(b) If two different phrases are to remain, should the definitions of "publicly available information" and "generally available information" be clarified in the legislation?

ISSUE 8

(a) Should the exemptions in any or all of the following provisions remain or are they made unnecessary by s 20(5) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 22(3) of the *Health Records and Information Privacy Act 2002* (NSW) and Schedule 1 to the *Freedom of Information Act 1989* (NSW):

- **s 4(3)(e)of the Privacy and Personal Information Protection Act 1998 (NSW) and s 5(3)(h) of the Health Records and Information Privacy Act 2002 (NSW);**
- **s 4(3)(i) of the Privacy and Personal Information Protection Act 1998 (NSW) and s 5(3)(l) of the Health Records and Information Privacy Act 2002 (NSW); and/or**
- **s 4(3)(ja) of the Privacy and Personal Information Protection Act 1998 (NSW)?**

(b) If any or all of the exemptions are to remain, should the information referred to in each provision be exempt from all the IPPs and HPPs or only some of them? Which, if any, IPPs and HPPs should apply to the information?

(c) If the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) are merged into one Act, how should the exemptions be worded if they are retained?

ISSUE 9

What is the rationale behind, and value of, the exception contained in s 4(3)(h) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(3)(k) of the *Health Records and Information Privacy Act 2002* (NSW) (information arising out of a complaint about conduct of police officers)?

ISSUE 10

Should a person who has made a complaint about police conduct be precluded from having access to their personal file in relation to the complaint process?

ISSUE 11

Should the police officer who is the subject of a complaint be able to access the information relating to the complaint?

ISSUE 12

Should some IPPs and HPPs but not others apply to information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990* (NSW)? If so, which ones should apply?

ISSUE 13

(a) Should the NSW Ombudsman be included among those agencies listed in s 27 of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 17 of the *Health Records and Information Privacy Act 2002* (NSW) as being exempt from compliance with the IPPs?

(b) Even if the answer to this is "yes", should the information referred to in s 4(3)(c), (d), (f) and (h) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(3)(f), (g), (i) and (k) of the *Health Records and Information Privacy Act 2002* (NSW) continue to be exempt from the definition of "personal information"?

ISSUE 14

Should the legislation continue to exempt from the definition of "personal information" information about an individual's suitability for appointment or employment as a public sector official?

ISSUE 15

Should the exemption from the definition of "personal information" of information about an individual's suitability for appointment or employment as a public sector official be restricted to information about a prospective employee, or also apply to information about an agency's current employee?

ISSUE 16

Do s 4(3)(j) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(3)(m) of the *Health Records and Information Privacy Act 2002* (NSW) need amending to clarify their meaning and Parliament's intention?

ISSUE 17

Should s 4(3)(j) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(3)(m) of the *Health Records and Information Privacy Act 2002* (NSW) be reworded to provide that they apply only to information that directly relates to suitability for recruitment, promotion, discipline and involuntary retirement?

ISSUE 18

(a) Should information contained in photographs or video images come within the definition of "personal information"?

(b) Should this depend on whether an individual's identity is apparent or can reasonably be identified from the visual image?

(c) If the definition of "personal information" should include visual images, should this be clarified in the legislation?

(d) Should some of the IPPs, but not others, apply to visual images that contain personal information? If so, which ones should apply?

ISSUE 19

(a) Should the meaning of the phrase "or can reasonably be ascertained from the information or opinion" in s 4(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 5(1) of the *Health Records and Information Privacy Act 2002* (NSW) be clarified?

(b) If so, should this be by an amendment to the legislation or should it be left to judicial construction or the publication of a Privacy Guideline?

Definition of "public sector agency" - PPIPA s 3(1); HRIPA s 4(1)

5.51 Sections s 3(1)(b) of PPIPA and s 4(1) of HRIPA provide that "public sector agency" includes "a statutory body representing the Crown". The Crown Solicitor has suggested that, since the decision in *McNamara v Consumer Trader and Tenancy Tribunal* ("*McNamara*"),[63] it is arguable that "a statutory body representing the Crown" is limited to those bodies that are expressly described in other Acts as such or declared to be "a NSW Government agency".[64] If, then, a body established for a public purpose by or under legislation falls outside s 3(1)(b), and cannot be described as any of the entities covered by sub-sections (a), (c), (e), (f) or (g), the Crown Solicitor argues that it is difficult to ascertain whether that body is intended to be a public sector agency. This is because the only sub-section left, sub-section (d), is difficult to apply as it requires complicated analysis of the auditing requirements of the *Public Finance and Audit Act 1983* (NSW).[65]

5.52 The Commission queries whether the decision in *McNamara* extends to support this argument. In *McNamara*, the Roads and Traffic Authority sought to claim the immunity conferred on the Crown in s 5 of the *Landlord and Tenant* (*Amendment) Act 1948* (NSW) by virtue of being "a statutory body representing the Crown". The High Court held that defining an agency in an Act as "a statutory body representing the Crown" did not automatically entitle that agency to the privileges and immunities of the Crown.[66] Crown immunity would need to be expressly given by the statute, or the statute could expressly define "Crown" so as to include "any statutory body representing the Crown".[67] Even so, it is arguable that, irrespective of *McNamara*, a "statutory body representing the Crown" would need to be declared as such by the statute creating its existence.

5.53 The Commission is also not convinced of the difficulty in establishing whether a person's or body's accounts are part of the accounts prepared under the *Public Finance and Audit Act 1983*

---

63. *McNamara v Consumer Trader and Tenancy Tribunal* (2005) 221 CLR 646.
64. Crown Solicitor 's Office, New South Wales, *Submission*, [3.1].
65. Crown Solicitor 's Office, New South Wales, *Submission*, [3.3].
66. See the minority decision in *Wynyard Investments Pty Ltd v Commissioner for Railways* (*NSW)* (1955) 93 CLR 376.
67. See *McNamara v Consumer Trader and Tenancy Tribunal* (2005) 221 CLR 646, [33] (McHugh, Gummow, Heydon JJ). However, in New South Wales the issue is now expressly clarified by s 13A of the *Interpretation Act 1987* (NSW), inserted into the Act in 2006 (*Interpretation Amendment Act 2006* (NSW)). This section states that if an Act provides that a body is a New South Wales Government agency, or a statutory body representing the Crown, the body has the status, privileges and immunities of the Crown.

(NSW), or whether they are required to be audited by the Auditor-General.

5.54 Nevertheless, the Commission sees merit in clarifying the status under PPIPA and HRIPA of bodies established for a public purpose but not expressly described in legislation as such or declared to be "a NSW Government agency". The Crown Solicitor has suggested that the definition in s 3(1)(b) of PPIPA and s 4(1) of HRIPA of a "public sector agency" as a "statutory body representing the Crown" should be defined either as "a body established or appointed for a public purpose by or under a NSW enactment" or, alternatively, "any public authority constituted by or under an Act".

5.55 The NSW Department of Health has pointed out that neither of these definitions may cover affiliated health organisations.[68] These are private benevolent organisations that receive 100% of their funding from the government, such as St Vincent's Hospital in Sydney and the Royal Flying Doctor Service.[69] They are significant service providers and record-keepers in the health sector and ought to be brought unambiguously within the scope of HRIPA.

ISSUE 20

Should s 3(1)(b) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to define a "public sector agency" as "a body established or appointed for a public purpose by or under a NSW Act " or, alternatively, "any public authority constituted by or under a NSW Act"?

ISSUE 21

Should s 4(1) of the *Health Records and Information Privacy Act 2002* (NSW) be amended to define a "public sector agency" as "a body established or appointed for a public purpose by or under a NSW Act or an affiliated health organisation" or, alternatively, "any public authority constituted by or under a NSW Act or an affiliated health organisation"?

Unsolicited information – PPIPA s 4(5); HRIPA s 10

5.56 Pursuant to s 4(5) of PPIPA and s 10 of HRIPA "personal information" under PPIPA and "health information" under HRIPA is

---

68. NSW Department of Health, *Consultation* (3 December 2007).
69. Section 13 of the *Health Service Act 1997* (NSW) describes "affiliated health organisations" as "certain non-profit, religious, charitable or other non-government organisations and institutions to be treated as part of the public health system where they control hospitals, health institutions, health services or health support services that significantly contribute to the operation of that system".

not "collected" by a public sector agency or organisation if receipt of the information by the agency/organisation is unsolicited. The consequence of this is that at least IPPs 1, 2, 3 and 4,[70] and HPPs 1, 2, 3 and 4, which regulate collection of information, and possibly other IPPs and HPPs, do not apply to unsolicited information.

5.57 There are two issues that arise here that make it difficult to delineate the scope of the exemptions under s 4(5) of PPIPA and s 10 of HRIPA. First, when is information "unsolicited"? Secondly, if it is unsolicited, what IPPs or HPPs do not then apply to that information? The legislation does not make this explicit.

5.58 In regard to the first issue, there is a lack of consensus between the cases decided by the ADT.[71] In *KD v Registrar, New South Wales Medical Board*, the ADT found that the applicant's complaint to the New South Wales Medical Board was unsolicited and therefore not "collected" under PPIPA and further observed that "virtually all complaints received by investigative agencies will be unsolicited".[72] Privacy NSW, however, has warned agencies against treating complaints to them as unsolicited if the agency holds itself out as the appropriate body to contact in the event of dissatisfaction.[73]

5.59 In *KD v Registrar, New South Wales Medical Board*, the ADT, having found that the information was unsolicited, found that IPPs 1, 2, 3 and 4 had no application.[74] In relation to the remaining IPPs, the Privacy Commissioner argued that IPPs 5-12[75] applied to personal information held by agencies, irrespective of whether that information was collected, within the meaning of PPIPA. That is, once an agency "holds" personal information, s 12-19 come into play.[76] The ADT held that while s 19 (IPP 12 – special restrictions on disclosure of personal information) catches all personal information held by an agency, however obtained, s 17 and 18 do not (IPPs 10 and 11 – limits on use and disclosure).[77] It held that it is implicit from the construction of

---

70. *Privacy and Personal Information Protection Act 1998* (NSW) s 8, 9, 10 and 11.
71. See A Johnston, *PPIPA in Practice: An Annotated Guide to the Privacy and Personal Information Protection Act 1998 (NSW)*, [28].
72. *KD v Registrar, New South Wales Medical Board* [2004] NSWADT 5, [27].
73. Privacy NSW, *Consultation* (2 July 2007).
74. *Privacy and Personal Information Protection Act 1998* (NSW) s 8, 9, 10 and 11.
75. *Privacy and Personal Information Protection Act 1998* (NSW) s 12, 13, 14, 15, 16, 17, 18 and 19.
76. *KD v Registrar, New South Wales Medical Board* [2004] NSWADT 5 [28].
77. *KD v Registrar, New South Wales Medical Board* [2004] NSWADT 5 [29]. See also *HW v Director of Public Prosecutions (No 2)* [2004] NSWADT 73.

these provisions that each applies only to information that has been collected.[78]

5.60 The Government, in its response to the Attorney General's statutory review of PPIPA, argued that where information is provided gratuitously and is not relevant to the function of the agency, it could be regarded as unsolicited and that, in such a case, it was difficult to see why an agency should be subjected to the same restrictions as for solicited material.[79] It concluded that the meaning of "unsolicited" needs further review. The statutory review recommended that PPIPA be amended to clarify that, while unsolicited information is not subject to the collection principles, the other IPPs do apply.[80] The Government neither supported nor rejected this recommendation but stated that it required further consideration.

5.61 The ADT's submission to the statutory review queried whether its decision in *KD v Registrar, New South Wales Medical Board* gave a degree of operation to the "unsolicited information" exception that was unintended.[81] It emphasised that an agency should not be exposed to the risk of contravening those IPPs that were formulated to protect a person from whom the agency actively sought information.[82] However, once the agency is in possession of the information, in the ADT's view,

---

78. "Section 17 refers to information held for a purpose 'other than that for which it was collected.' This seems to me to confine the relevant information to information that had been collected by the agency for one purpose and prevents it being used for another. Critically, it relates to collected information. The interpretation of s 18 is more difficult but I think that the same implication obtains. Section 18(1)(a) again refers to the purpose for which information has been collected. Sub-section (1)(b) refers to personal information "of that kind" held by an agency. I think that there is a reasonable inference that this refers to "collected information" also, although it is not as clear in this instance as in (1)(a). It may well also refer to the wider category of unsolicited information. Given that this is beneficial legislation, s 18(1)(b) ought be given the wider interpretation. That view is strengthened by the fact that s 18(2) refers to 'the purpose for which the information was given to it' rather than, as in s 18(1)(a), 'for which the information was collected'.": *KD v Registrar, New South Wales Medical Board* [2004] NSWADT 5, [29].
79. New South Wales Government, *Response to the Report on the Statutory Review of the Privacy and Personal Information Protection Act 1998*, 8.
80. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, Recommendation 16.
81. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 9.
82. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 10. For example, IPPs relating to notice of purpose of collection and intended uses of the information.

the agency should comply with the IPPs relating to security, use, disclosure, access and amendment.[83] The ADT went on to argue that:

> according to *KD*, important limits that have been placed on use and disclosure may not apply because they only relate to information that has been "collected" and that term does not cover unsolicited information. This is a perverse result. It should be made clear that unsolicited information is not affected by the Collection principles but is otherwise subject to PPIPA.[84]

ISSUE 22

Should the meaning of "unsolicited" in s 4(5) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 10 of the *Health Records and Information Privacy Act 2002* (NSW) be clarified?

ISSUE 23

If information is "unsolicited", what IPPs or HPPs, if any, should apply to that information? Should all of the provisions of the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) apply to unsolicited information, except the collection IPPs and HPPs?

Law enforcement and investigative agencies – PPIPA s 23, 24 and 27; HRIPA s 27

5.62 Sections 23 and 24 of PPIPA exempt law enforcement agencies and investigative agencies from having to comply with certain of the IPPs if, generally speaking, the information relates to, or compliance with the sections interferes with, the agencies' law enforcement, investigative or complaints-handling functions. Section 27 of PPIPA and s 17 of HRIPA specifically exempt the Independent Commission Against Corruption, the Police Service (NSW Police), the Police Integrity Commission and the NSW Crime Commission from compliance with all of the IPPs in PPIPA's case,[85] and compliance with the Act as a whole, in HRIPA's case, unless the information is in

83. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 10.
84. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 10.
85. *Privacy and Personal Information Protection Act 1998* (NSW), s 27(1).

connection with the exercise of their "administrative and educative functions".[86]

5.63 This "administrative and educative functions" rider to the exemption ostensibly lessens the impact of the exemption itself on privacy protection. However, three aspects of its application may undermine this. First, the meaning of "administrative function" is not settled and may be construed more narrowly than Parliament intended. Secondly, a function may have a dual character, possessing both administrative and non-administrative purposes. For example, an administrative function may only be carried out as incidental to a non-administrative function, or necessary to ensure its effective exercise. In that case, the non-administrative function may not be isolated, with the application of IPPs to it, but be subsumed into the operational function. Related to this, if a function cannot easily be categorised as administrative or educative, it may automatically be categorised as operational, thereby coming within the exemption. This categorisation by default broadens the scope of s 27 of PPIPA and s 17 of HRIPA.

5.64 The difficulty faced in distinguishing administrative functions from operational functions is illustrated in *YK v Commissioner of Police, NSW Police*.[87] The applicant in that case, YK, complained to the ADT that a NSW Police officer had breached PPIPA by revealing to YK's employer, NSW Health, information collected by the police in the course of their investigations into child sexual assaults allegedly committed by YK. NSW Police claimed that the conduct was exempt from the IPPs pursuant to s 27 because the information was disclosed in the course of carrying out its investigative functions.

5.65 The ADT referred to the decision of *HW v Commissioner of Police, NSW Police Service*, in which the Tribunal had said that s 27 sought "to draw a distinction between the core responsibility of the Police Service and its 'administrative' and educative' functions".[88] Having divided responsibilities into core and non-core, the ADT held that the meaning of "administrative" in s 27 should "be read down so as not to embrace those core responsibilities".[89] It could not be used "to refer to the entirety of the administrative activity of the Police Service, which includes the investigation of a crime" but refers "to those activities that have to do with providing administrative support

86. *Privacy and Personal Information Protection Act 1998* (NSW), s 27(2).
87. *YK v Commissioner of Police, New South Wales Police* [2008] NSWADT 81.
88. *HW v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 214, [25].
89. *HW v Commissioner of Police, New South Wales Police Service & Anor* [2003] NSWADT 214, [27].

for the conduct of its core responsibilities".[90] The ADT also acknowledged, however, that characterisation of some activities "in terms of core/administrative/educative may vary depending on the context that has given rise to the conduct in issue".[91]

5.66 In the case before it, the ADT stated that the characterisation of the conduct as core or administrative was "ultimately a question of fact having regard to the circumstances in which the disclosure was made".[92] The ADT found that the disclosure of personal information about YK was made years after the assaults allegedly occurred and after NSW Police had completed its investigations and determined that there was insufficient evidence to prosecute, and were made to NSW Health to assist it in assessing YK as an employee. In those circumstances, the ADT held that the disclosure was made pursuant to "administrative" functions.[93] The facts of the case were complicated by a request to NSW Police from the Ombudsman for information about the allegations, the Ombudsman having become aware of the allegations through NSW Health. The case illustrates the difficult exercise that an agency (or the tribunal or the Privacy Commissioner if a complaint is made) must embark on to establish whether information can lawfully be exempted from the IPPs under s 27.

5.67 Lastly, agencies/organisations may themselves avoid categorising functions as administrative or educative in order to by-pass the application of IPPs to information collected in relation to them, or, in the case of health organisations, to avoid the application of HRIPA altogether.

5.68 The purpose of the exemption is to achieve "balance between the competing interests of the need for privacy protection of government-held information bases and the need for a reasonable flow of information for valid purposes of investigation and law enforcement".[94]

5.69 In order to facilitate investigation and law enforcement, s 27 of PPIPA and s 17 of HRIPA contain legitimate and necessary exemptions. The issue arises, however, as to whether the "administrative and educative functions" rider to the exemption has

---

90. *HW v Commissioner of Police, New South Wales Police Service & Anor* [2003] NSWADT 214, [29].
91. *HW v Commissioner of Police, New South Wales Police Service & Anor* [2003] NSWADT 214, [30].
92. *YK v Commissioner of Police, New South Wales Police* [2008] NSWADT 81, [26].
93. *YK v Commissioner of Police, New South Wales Police* [2008] NSWADT 81, [33].
94. New South Wales, *Parliamentary Debates,* Legislative Council, Second Reading Speech, 14 October 1998, 8251 (the Hon J W Shaw).

been weakened in practice so as to upset the balance of which the Attorney General spoke. The Privacy Commissioner pointed out to the review of PPIPA that the Government's purpose in enacting s 27 was "not to protect secrecy in dealings or to protect the Government from accountability"[95] and submitted that, in keeping with this, the exemption should be defined more closely.[96]

ISSUE 24

Should the meaning of, and distinction between, "administrative" and "educative" functions in s 27 of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 17 of the *Health Records and Information Privacy Act 2002* (NSW) be more clearly defined?

ISSUE 25

Should the legislation explicitly provide that if a function is dual, the administrative function must be separately categorised?

ISSUE 26

Is the opportunity to complain to the Privacy Commissioner and challenge the categorisation of a function sufficient?

State owned corporations

5.70 PPIPA specifically excludes State owned corporations ("SOCs") from the definition of "public sector agency". Accordingly, twenty-one corporatised government agencies, including Sydney Ferries, Railcorp, Sydney Water, NSW Lotteries, Landcom, Energy Australia and Integral Energy, are not regulated at all by PPIPA.[97]

5.71 The exclusion of SOCs from the scope of PPIPA was vigorously debated during the passage of the legislation through New South Wales Parliament in 1998. The Opposition in the Legislative Council moved an amendment to bring SOCs within the statute's ambit. The then Shadow Attorney General, the Hon J Hannaford, MLC, argued that all SOCs are "organs of the State" and are Government agencies that have been "corporatised to drive efficiencies within that

95. New South Wales, *Parliamentary Debates,* Legislative Council, Second Reading Speech, 14 October 1998, 8251 (the Hon J W Shaw).
96. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998*, 74.
97. See *State Owned Corporations Act 1989* (NSW) sch 5 for a list of all statutory State owned corporations.

agency".[98] He concluded that "[a]dherence to privacy principles should not affect that efficiency".[99] Further, he noted that the 1992 report by the Independent Commission Against Corruption on the unauthorised release of Government information cited SOCs as "amongst the worst offenders" in terms of selling private information.[100]

5.72 In response, the then Attorney General, the Hon J W Shaw, QC, MLC noted that including SOCs within the scope of PPIPA would place them at a "competitive disadvantage" with the private sector, which, in 1998, had not yet been regulated by privacy legislation.[101] The former Attorney General recognised the desirability of extending privacy laws to the private sector, but considered that this should be done at a national, rather than State, level.[102] The intention was for SOCs to be covered by privacy legislation at a future time, when the rest of the private sector was similarly covered. The proposed amendment was passed in the Legislative Council, but overturned in the Legislative Assembly.

5.73 The *Privacy Amendment* (*Private Sector) Act 2000* (Cth) began operation on 21 December 2001. That Act incorporated into the *Privacy Act 1988* (Cth) 10 National Privacy Principles, which must be followed by private sector organisations as defined in the legislation. The definition of "organisation" in the Commonwealth Act specifically excludes State or Territory authorities and instrumentalities.[103] However, a separate section of the *Privacy Act 1988* (Cth) provides that those authorities or instrumentalities may be covered by the Act if prescribed in the regulations made under the legislation.[104] The *Privacy* (*Private Sector) Regulations 2001* (Cth) prescribes four SOCs as organisations for the purposes of the *Privacy Act 1988* (Cth). They are:

- Australian Inland Energy Water Infrastructure;
- Country Energy;
- Energy Australia; and

---

98. New South Wales, *Parliamentary Debates,* Legislative Council, 28 October 1998, In Committee, 9151-9152 (the Hon J Hannaford).
99. New South Wales, *Parliamentary Debates*, Legislative Council, 28 October 1998, In Committee, 9151-9152 (the Hon J Hannaford).
100. New South Wales, *Parliamentary Debates*, Legislative Council, 25 November 1998, In Committee, 10562 (the Hon J Hannaford).
101. New South Wales, *Parliamentary Debates,* Legislative Council, 28 October 1998, In Committee, 9152 (the Hon J Hannaford).
102. New South Wales, *Parliamentary Debates,* Legislative Council, 17 September 1998, Second Reading Speech, 7601 (the Hon J W Shaw).
103. See *Privacy Act 1988* (Cth) s 6C.
104. *Privacy Act 1988* (Cth) s 6F.

- Integral Energy.[105]

5.74 Therefore, the personal information held by the remaining 17 SOCs listed in Schedule 5 to the *State Owned Corporations Act 1989* (NSW) is not regulated either by the Commonwealth Privacy Act or by PPIPA. Those organisations (as well as the four listed above) are, however, covered under HRIPA in relation to any health information they hold concerning employees.

5.75 The Government's original intention in excluding SOCs from PPIPA "to ensure a level playing field"[106] is no longer valid. Secondly, there is no even-handedness in the patchwork coverage of SOCs by privacy legislation that now prevails. Thirdly, the current approach of privacy legislation to SOCs is not consistent with the principal objectives of SOCs prescribed by s 20E of the *State Owned Corporations Act 1989* (NSW). These include: to be a successful business and, to this end, to operate at least as efficiently as any comparable businesses;[107] and to exhibit a sense of social responsibility by having regard to the interests of the community in which it operates.[108]

5.76 In relation to the first objective, bringing some SOCs under the jurisdiction of privacy legislation but not others may make it harder for certain SOCs to operate as efficiently as comparable businesses not bound by privacy obligations. In relation to the second objective, a SOC that is immune from privacy obligations is not fully exhibiting a sense of social responsibility in that area. Being aware of this shortcoming, Sydney Water voluntarily complies with the IPPs "as a matter of customer respect and trust".[109]

5.77 Some SOCs indicated to the Attorney General's review of PPIPA that they wanted to be covered by the Commonwealth *Privacy Act 1988* in order to take advantage of exemptions relating to the transfer of personal information between agencies.[110]

5.78 The Commission is of the view that all SOCs should be covered by privacy legislation, whether by PPIPA or the *Privacy Act 1988* (Cth), providing there is no duplication of coverage.

---

105. *Privacy (Private Sector) Regulations 2001* (Cth) cl 3A.
106. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [9.29].
107. *State Owned Corporations Act 1989* (NSW) s 20E(1)(a)(i).
108. *State Owned Corporations Act 1989* (NSW) s 20E(1)(b).
109. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [8.7].
110. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [8.8].

PROPOSAL 6

All State owned corporations should be covered by privacy legislation.

Government contractors

5.79 While PPIPA specifically excludes SOCs from the definition of "public-sector agency", the Act is silent on the status of non-government organisations contracted by public-sector agencies to provide services to the public. To come within PPIPA's ambit, government contractors would have to be specifically included by the legislation, as it would be straining statutory interpretation to define government contractors as "public sector agencies".

5.80 There is clearly a disparity in government contractors, standing in the shoes of a public sector agency, having no obligations to protect the privacy of the personal information of the customers with whom they deal. For example, all insurers contracted to Workcover are private and Privacy NSW reports that there are numerous complaints about breaches of privacy by these insurers. They are not bound by the IPPs and there is no internal review of conduct.

5.81 Both the Commonwealth and Victorian jurisdictions have seen fit to regulate protection of information privacy where a public sector agency has contracted the services of a private organisation. Section 95B(1) of the *Privacy Act 1988* (Cth) provides that the agency must "take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an [IPP] if done or engaged in by the agency". Section 17 of the *Information Privacy Act 2000* (Vic) provides that "a State contract may provide for the contracted service provider to be bound by the [IPPs] and any applicable code of practice … in the same way and to the same extent" as the public sector agency itself would have been bound if it had provided the service directly.

5.82 Privacy NSW has argued that PPIPA should include a mandatory requirement binding contractors to the same privacy standards, being the applicable IPPs and any modifications under a privacy code of practice, as apply to the agency itself.

5.83 The Attorney General's review of PPIPA recommended that PPIPA should provide a structure to bind government contractors providing services that require management of personal information, so as to "conform to the terms" of PPIPA, unless they are otherwise bound by equivalent privacy laws.[111]

---

111. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, Recommendation 13.

5.84 The Commission agrees with this recommendation and the view of Privacy NSW and accordingly makes the following proposal.

PROPOSAL 7

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that where a public sector agency contracts with a non-government organisation to provide services for government, the non-government organisation should be contractually obliged to abide by the IPPs and any applicable code of practice in the same way as if the public sector agency itself were providing the services.

SHOULD OTHER ASPECTS OF PRIVACY BE EXPRESSLY PROTECTED IN PPIPA?

Background

5.85 PPIPA deals primarily with safeguarding information privacy. It is clear from the Parliamentary debates that saw the passage of the *Privacy and Personal Information Protection Bill* through both Houses that the focus was on data protection. However, there is in PPIPA protection of other facets of privacy. The purpose of the Act is generally "to promote the protection of privacy and the rights of the individual"[112] and the Privacy Commissioner is given a general power to "receive, investigate and conciliate complaints about privacy related matters".[113] In addition, s 45(1) of PPIPA provides that complaints may be made to (or by) the Privacy Commissioner about the alleged violation of, or interference with, the privacy of the individual.[114] That PPIPA offers general privacy protection is clear, but the scope of this protection is indeterminate.

5.86 The second aspect of PPIPA's general privacy protection is that the only remedy available to a complainant is conciliation by the Privacy Commissioner. If the alleged transgressor of physical privacy is a public sector agency, there is no right of internal review and subsequent appeal to the ADT.

5.87 This section considers whether the scope of the legislation can be amplified by giving express and defined protection to more general aspects of privacy, in particular, physical privacy, and by offering a wider range of remedies to redress invasions of privacy.

---

112. *Privacy and Personal Information Protection Act 1998* (NSW), Long Title. See also New South Wales, *Parliamentary Debates,* Legislative Council, 17 September 1998, Second Reading Speech, 7600 (the Hon J W Shaw).
113. *Privacy and Personal Information Protection Act 1998* (NSW), s 36(2)(k).
114. The Commissioner may also make a complaint on his or her own initiative: *Privacy and Personal Information Protection Act 1998* (NSW), s.45(1).

What are "privacy related matters"?

5.88 There is no guidance in the Act as to what "privacy related matters" might appropriately fall within the scope of s 36(2)(k). In investigating a complaint, Privacy NSW relies, initially at least, on what is termed "the Prosser test".[115] This is a standard based on:

- the intrusion upon the plaintiff's seclusion or solitude, or into his or her private affairs;
- public disclosure of embarrassing facts about the plaintiff;
- publicity that places the plaintiff in a false light in the public eye; and
- appropriation of the plaintiff's name or likeness.

5.89 Any strengthening of the protection of privacy in PPIPA need not, of course, be bound by the current phrase "privacy related matters", or by the Prosser test of invasion of privacy. One way to approach the issue of general privacy protection in PPIPA is for the legislation to attempt to identify a universal notion of privacy, such as "the right to be let alone", or some other concept crafted around an individual's right to "dignity" or "autonomy". This, however, presents a considerable philosophical challenge – one which the Commission grappled with in its Consultation Paper 1, *Invasion of Privacy* ("CP 1").[116]

5.90 A different, more pragmatic, approach is to identify categories of privacy in order to imbue the term with a workable meaning. CP 1 illustrated this approach by reference to the categories of privacy identified by Privacy International,[117] namely:

- information privacy, or data protection;

---

115. The Office of the New South Wales Privacy Commissioner, *Protocol for the Handling of Complaints by Privacy NSW* (22 July 2002, revised July 2006), [2.3.2.3]. The "Prosser Test" is the standard described in the 1973 Report to the New South Wales Parliament on the Law of Privacy: W L Morison, *Report on the Law of Privacy* (No 170, Parliament of New South Wales, 1973), [22]-[23]. In that report, Professor Morison referred extensively to the United States tort of privacy authoritatively summarised by Dean William L Prosser: W L Prosser, "Privacy" (1960) *California Law Review* 48, 383. See New South Wales Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007), Ch 4 for an extensive discussion of the Prosser Test and of the law of privacy protection in the United States.
116. NSWLRC CP 1, [1.12-1.18]. See also Australian Law Reform Commission, *Review of Privacy* (Discussion Paper 72, 2007), [1.29]-[1.63].
117. Privacy International, *Privacy and Human Rights 2000 Overview* *http://www.privacyinternational.org/survey/phr2000/overview.html* at 7 February 2008.

- bodily privacy, including protection against invasive procedures and DNA testing;
- privacy of communications, covering security of electronic and standard mail and telephone communications; and
- territorial privacy, covering surveillance and protection against other intrusions into people's physical space.

5.91 A refinement of this approach identifies categories of activity that have the potential to breach privacy. The four categories identified by Solove are:

- information collection, including surveillance and interrogation;
- information processing;
- information dissemination; and
- intrusion.[118]

5.92 It may not, therefore, be necessary to settle on a definition of privacy for the purposes of reforming PPIPA, but simply to draw on areas of activity that the legislation could regulate. Referring back to Privacy International's categories of privacy, privacy beyond information privacy can involve bodily privacy, privacy of communications and territorial privacy.

Bodily privacy

5.93 The main areas of protection in this category are in relation to invasive procedures and genetic testing. What is relevant here is the actual physical privacy afforded an individual, not the privacy of personal information collected as a result of genetic testing or other medical procedures, or contained in genetic and other bodily samples. The privacy of personal information in the form of body samples or genetic characteristics is governed by HRIPA.

5.94 The issue that arises is whether PPIPA can effectively, and appropriately, offer protection to an individual whose bodily privacy has been invaded, or whether this is not better dealt with by specific legislation.

5.95 For example, the *Human Tissue Act 1983* (NSW) regulates donation of tissue (including blood and semen) by living persons, removal of tissue from deceased persons and the conduct of post-mortem examinations. It governs such things as issues of consent and use of tissue removed during medical, dental or surgical treatment.

---

118. D J Solove, "A Taxonomy of Privacy" (2006) 154 *University of Pennsylvania Law Review* 477, 488-489. See NSWLRC CP `1 [1.17]-[1.18].

Another example of specialised legislation in the area of bodily privacy is the *Crimes* (*Forensic Procedures) Act 2000* (NSW). This Act regulates the carrying out of forensic procedures on criminal suspects, convicted offenders and other persons, and the retention, admissibility and destruction of forensic material. It also regulates storage of information on a DNA database. An example of specialised legislation at the Commonwealth level is the *Genetic Privacy and Non-discrimination Bill 1998*. If enacted, it would protect the genetic privacy of individuals, prohibit genetic discrimination and provide for the collection, storage and analysis of DNA samples.[119]

5.96 At this point, the Commission is leaning towards the view that such a complex and specialised area as bodily privacy is best regulated by dedicated legislation that covers all aspects of the subject matter, including privacy, consent, authority to collect and use, and so forth. Provisionally, this approach appears to be preferable to bringing bodily privacy under the umbrella of PPIPA. However, the Commission would like to receive submissions on this issue.

ISSUE 27

Should the *Privacy and Personal Information Protection Act 1998* (NSW) contain express provisions for the general regulation of bodily privacy?

Privacy of communications

5.97 Privacy of communications covers the security of standard mail and electronic communications. Electronic communications include computer communications such as email, electronic data interchange, “chat room” correspondence, instant messaging, mobile phone calls and messaging, PDA communications and landline telephone calls.

5.98 The *Telecommunications* (*Interception and Access) Act 1979* (Cth) prohibits, except where specifically authorised, two main heads of conduct: (1) the interception of communications passing over a telecommunication system;[120] and (2) access to stored communications. “Communication” is defined to include conversations or messages in the form of speech, music or other sounds, data, text, visual images or signals, or in any other form or combination of forms.[121] A “stored communication” is a communication that: is not passing over a

119. This may not, however, come to pass as the Bill was introduced into the Commonwealth Parliament in 1998, restored in 2004, but lapsed again on 15 October 2007.
120. *Telecommunications* (*Interception) Act 1979* (Cth) s 7.
121. *Telecommunications* (*Interception) Act 1979* (Cth) s 5. The definition of “interception” refers only to “listening to or recording” such communications: s 6.

telecommunications system; is held on equipment operated by and in the possession of a carrier; and cannot be accessed by a third party without the carrier's assistance. Accessing a stored communication means listening to, reading or recording it by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.

5.99 The *Telecommunications* (*Interception and Access) Act 1979* (Cth) was amended in 2006 to add the prohibition on accessing stored communications.[122] Case law prior to the 2006 amendment held, in relation to telephone interceptions, that the *Telecommunications* (*Interception) Act 1979* (Cth) was intended to cover the field, thus displacing any State legislation that might otherwise apply.[123] It is probable, although not entirely clear, that the courts would also have held that all other types of communications intercepted during their passage across a telecommunications system would have been regulated exclusively by the *Telecommunications* (*Interception) Act 1979* (Cth). This Constitutional issue has not been tested in the courts in relation to the *Telecommunications* (*Interception and Access) Act 1979* (Cth) but there is no evidence to suggest that the amendment changes the Commonwealth's intention that the Act should cover the field. For that reason, it is difficult to see how PPIPA/HRIPA could include provisions that regulate the privacy of telecommunications.

5.100 The privacy of information that is obtained by telecommunications providers is a separate, albeit related, issue and not relevant to the present discussion. Use and disclosure of that information is regulated by the Commonwealth *Telecommunications Act 1997* and must remain in the federal domain.

Territorial privacy

5.101 Territorial privacy covers surveillance and protection against other intrusions into people's physical space. A large number of complaints received by the Privacy Commissioner relate to the use of Closed Circuit Television (CCTV). For example, Privacy NSW has investigated a number of complaints that neighbours are training cameras on the complainant's property (sometimes with both audio and video surveillance mechanisms), filming the complainant, and often the complainant's children, going about their business in their

122. *Telecommunications* (*Interception) Amendment Act 2006* (Cth). The name of the Act was also changed from the *Telecommunications* (*Interception) Act 1979* (Cth) to its present name, the *Telecommunications* (*Interception and Access) Act 1979* (Cth) to reflect its expanded scope.

123. *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222 at 230; *Miller v Miller* (1978) 141 CLR 269. See *Constitution Act* s 109.

own home and backyard.[124] This is apparently being done to harass or intimidate the complainant,[125] or as revenge in the context of neighbour-neighbour disputes.

5.102 Because the cameras are fixed on the neighbour's own private property, there is nothing that Privacy NSW can do to remedy the situation. There is no specific legislation regulating surveillance in residential settings. As its name makes clear, the *Workplace Surveillance Act 2005* (NSW) only regulates surveillance in a workplace, prohibiting covert surveillance of employees in the workplace without appropriate notice. For surveillance outside the workplace, the complainant's only options are to bring an action in nuisance,[126] involving costly litigation with an uncertain outcome, or to seek an Apprehended Violence Order. Again, success of this action is far from certain. The Crown needs to prove beyond reasonable doubt that the filming of the complainant amounts to harassment or molestation.[127]

5.103 In 2005, the Commission published its final report on surveillance. The Commission recommended the enactment of a *Surveillance Act* to regulate all overt and covert surveillance activity in New South Wales.[128] Under the proposed Act, the Privacy Commissioner would have an important role in the regulation of overt surveillance.[129] Although the Government has indicated that it will not be implementing the recommendation, the Commission stands by its conclusions and recommendations, and its preferred position continues to be that surveillance be regulated under a dedicated *Surveillance Act*. Issues arising out of surveillance are separate from issues relating to information privacy, and should be kept separate. However, we invite submissions addressing the question whether territorial privacy should be protected in PPIPA.

ISSUE 28

Should the *Privacy and Personal Information Protection Act 1998* (NSW) contain express provision for breaches of territorial privacy?

124. See, for example, Privacy NSW, *Annual Report 2005-06* (2006), 28.
125. One complaint of surveillance of this nature, for example, arose out of the complainant's refusal to withdraw objections to the neighbour's Development Application.
126. See *Raciti v Hughes* (unreported, New South Wales Supreme Court, Young J, 3667 of 1995, 19 October 1995).
127. *Crimes Act 1900* (NSW) s 562D(1).
128. New South Wales Law Reform Commission, *Surveillance: Final Report* (Report 108, 2005); New South Wales Law Reform Commission, *Surveillance: An Interim Report* (Report 98, 2001).
129. NSWLRC Report 108, Recommendation 2.

A GENERAL CAUSE OF ACTION FOR INVASION OF PRIVACY?

5.104 The whole question of what aspects of privacy PPIPA should protect, and whether PPIPA should provide comprehensive remedies for breaches of privacy, is complicated by the possible enactment of a statutory cause of action for invasion of privacy.

5.105 The Commission published a consultation paper in May 2007 ("CP 1")[130] seeking comment on whether there should be a general cause of action for invasion of privacy and, if so, what the boundaries of that cause of action should be. How the provisions of PPIPA would dovetail with a statutory cause of action is crucial to the resolution of the issues raised above but the outcome of the enquiry set in train by CP 1 will not be known for some time. It will involve extensive research, consultation, deliberation of submissions and debate, and may or may not result in a statutory cause of action for invasion of privacy. If it does, what conduct would be covered, what remedies would be available, and which court or tribunal would have jurisdiction under the statute, is yet to be determined.

5.106 Having said that, because the two enquiries – this and CP 1 – have different emphases, it is possible to pursue an examination of the scope of privacy protection under PPIPA and HRIPA at this time. Put simply, PPIPA and HRIPA can be viewed as offering preventative, or "front-end", protection, while a statutory cause of action can be viewed as offering curative, or "back-end", protection. The schemes of PPIPA and HRIPA put in place a framework to ensure that information privacy is protected and to forestall breaches of privacy; whereas a statutory cause of action for invasion of privacy would offer redress for breaches, or invasions, of privacy that occur. There is, of course, overlap. PPIPA and HRIPA also offer mechanisms to deal with breaches of privacy; and a cause of action for invasion of privacy acts as a preventative measure in privacy protection by putting people on notice what conduct will and will not be tolerated by the law.

5.107 The second difference in emphasis between the two enquiries is on whom the duty of compliance falls. Other than s 45, which implicates all individuals and organisations in obligations to respect privacy, the provisions of PPIPA regulate public sector agencies. A statutory cause of action for invasion of privacy would not be likewise limited. It would apply to all individuals and bodies whether public or private. While HRIPA regulates both the public and private sectors, Chapter 4 raises the possibility, which the Commission favours, of transferring responsibility for private sector health service agencies and providers from New South Wales to the Commonwealth, leaving the State legislation applying to the public sector only.

130. NSWLRC CP 1.

5.108 Elements common to the two inquiries are the challenge of setting the boundaries of privacy protection and the appropriate remedies for breaches. The challenge lies both in determining the reach of a statutory cause of action and of PPIPA and resolving the overlap between the statutes. Although the overlap is reduced (to State authorities) if a statutory cause of action is enacted at both the federal and State levels, there is still a question of overlap with the rest of FOI legislation, meaning that an overlap with information privacy will continue to exist.

5.109 Simultaneously with this inquiry, the Australian Law Reform Commission ("ALRC") is conducting a review of Commonwealth privacy law. In its Discussion Paper 72,[131] it has combined the two equivalent phases of the Commission's review – the operation of existing privacy legislation and the possibility of a statutory cause of action for invasion of privacy - in the one discussion paper and has reconciled the two paths of inquiry in the following way. It proposes that a statutory cause of action be introduced at the federal level and that this be included in the *Privacy Act 1988* (Cth). The ALRC proposes that the *Privacy Act* would then cover: interference with an individual's home or family life; surveillance; and interference with, or misuse or disclosure of, correspondence or private written, oral or electronic communications.[132].

5.110 The Commission's final report will coalesce the responses to its CP 1, the ALRC's DP 72 and this paper to make recommendations that offer the best mechanisms for protecting, and redressing invasions of, all aspects of an individual's privacy, in a framework of harmonisation with the Commonwealth.

ISSUE 29

If a statutory cause of action for invasion of privacy is to be enacted, what should be its relationship be to the *Privacy and Personal Information Protection Act 1998* (NSW)?

131. ALRC DP 72.
132. ALRC DP 72, Proposal 5-1.

6. The privacy principles

- Introduction
- Collection for lawful purposes – IPP 1; HPP 1
- Collection directly from the individual – IPP 2; HPP 3
- Further collection requirements – IPP 3 and IPP 4; HPP 4
- Application of IPPs to records of observations or conversations
- Retention and security of information – IPP 5; HPP 5
- Access to, and alteration of, information – IPP 7 and IPP 8; HPP 8
- The dichotomy between “use” and “disclosure” – IPPs 9, 10, 11 and 12; HPPs 9, 10, 11 and 12
- Identification of the purpose for collection – IPPs 10 and 11; HPPs 10 and 11
- Application of IPPs 10 and 11 and HPPs 10 and 11 to unsolicited information
- Disclosure to third parties – IPP 11
- Special restrictions on disclosure – IPP 12
- Regulating unique identifiers

INTRODUCTION

6.1 This and the following chapter identify specific problems with the application of particular provisions of the *Privacy and Personal Information Protection Act 1998* (NSW) ("PPIPA") and the *Health Records and Information Privacy Act 2002* (NSW) ("HRIPA"). There is, however, overlap between this and the following chapter and Chapter 5. The three chapters should, therefore, be read together. For example, problems have arisen with a number of provisions that exempt certain information from the definition of "personal information" because they have been found to be too broad and/or imprecise. While these provisions are discussed in Chapter 5 in the context of the potential extension of the scope of PPIPA and HRIPA, they could also have appropriately been dealt with in this or the following chapter. Chapter 7 includes discussion of two exemptions arising from s 24 and 25 of PPIPA. The reason the exemptions have been evaluated in that chapter, and not included in the discussion of other exemptions in Chapter 5, is that the issues arising do not relate to extending the scope of PPIPA, the focus of Chapter 5. The issues relate to the functioning of the legislation. We raise concerns that there is a dichotomy in the way s 24 of PPIPA applies and an ambiguity in the application of s 25. If anything, resolution of the problems with these sections may result in a narrowing, rather than a widening, of PPIPA's application to personal information.

6.2 Many of the difficulties that agencies and the public experience in relation to the operation of privacy legislation arise out of the Privacy Principles. This chapter is, therefore, devoted to analysing these difficulties. Chapter 7 continues the examination of operational issues, focusing on issues relating to: s 37 and 38 of PPIPA; privacy codes of practice; public interest directions; complaints about, and review of, agency/organisation conduct; and s 24 and 25 of PPIPA, mentioned above.

6.3 PPIPA contains 12 Information Protection Principles ("IPPs") set out in Part 2, s 8-19 and HRIPA contains 15 Health Privacy Principles ("HPPs") set out in Schedule 1 to the Act. These are set out in detail in Chapter 3. The focus in submissions to the Commission has been on the IPPs and, obviously, submissions to the Attorney General's review of PPIPA focused on the IPPs. Accordingly, this consultation paper does not raise as many issues in relation to the HPPs as it does for the IPPs. The Commission intends to consult further with the Department of Health and other relevant bodies, following release of this paper, to inquire more extensively into how the HPPs are working in practice. We also welcome submissions on this subject.

COLLECTION FOR LAWFUL PURPOSES – IPP 1; HPP 1

6.4 IPP 1 (PPIPA s 8) and HPP 1 regulate the collection of personal information "for a lawful purpose" by reasonable means (PPIPA) or as reasonably necessary (HRIPA). Privacy NSW has recommended that IPP 1 be amended to include a specific limitation on the collection of sensitive classes of personal information.[1]

6.5 While there is no specific definition of "sensitive information" in PPIPA, s 19 refers to categories of information that can be taken to be sensitive information. That section (IPP 12) applies restrictions to the disclosure of "personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities". HRIPA does not refer to "sensitive information" at all.

6.6 Privacy NSW has submitted that the collection of particularly sensitive information should be more strictly regulated. It argues that, although IPP 12 regulates disclosure of such information, the best means of preventing misuse is to restrict its collection in the first place to that which is strictly necessary.[2]

6.7 The Department of Health disagrees with this view and is not persuaded that change is needed.[3]

6.8 The Unified Privacy Principles ("UPPs") proposed by the Australian Law Reform Commission ("ALRC")[4] bring together in one UPP, namely UPP 2, the collection privacy principles. The ALRC proposes, in UPP 2.6 that, "in addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual" unless certain conditions are met.[5] Generally speaking, consent to the collection from the individual is required, unless there are certain prevailing circumstances, including a serious threat to life or health.[6] There is no restriction on the collection of sensitive information to that which is strictly necessary.

1. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), 44.
2. Crown Solicitor 's Office, New South Wales, *Advice*, 43. See National Privacy Principle 10 in the *Privacy Act 1988* (Cth); IPP 10 in the *Information Privacy Act 2000* (Vic); and IPP 10 in the *Information Act* (NT).
3. NSW Department of Health, *Consultation* (3 December 2007).
4. See Australian Law Reform Commission, *Review of Privacy* (Discussion Paper 72, 2007), 89-100.
5. ALRC DP 72, 100.
6. Compare s 19 of the *Privacy and Personal Information Protection Act 1998* (NSW), which requires a serious *and imminent* threat to life or health before sensitive information can be *disclosed*.

ISSUE 30

Should IPP 1 be amended to include a provision that a public sector agency must not collect personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, sexual activities or criminal record (defined as "sensitive information") unless the collection is strictly necessary?

ISSUE 31

Should collection of sensitive information be allowed if necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person?

COLLECTION DIRECTLY FROM THE INDIVIDUAL – IPP 2; HPP 3

6.9 ***IPP 2*** (PPIPA s 9) provides that personal information must be collected directly from the individual to whom it relates unless that individual authorises indirect collection, or the information is about a child under the age of 16 and provided by a parent or guardian.

6.10 The Crown Solicitor has suggested that IPP 2 is one of the most difficult of the IPPs for agencies to comply with. Examples of situations that cause difficulties include where an individual is incapable of authorising collection from another person due to the individual's illness or mental disability or because the individual is deceased or missing. While s 26(1) exempts the agency from complying with s 9 if this "would, in the circumstances, prejudice the interest of the individual to whom the information relates", in many cases, it is difficult for agencies to know whether, or to assume that, compliance would result in such prejudice.[7]

6.11 Another example is where an agency seeks professional legal or financial advice and needs to disclose personal information to the professional in order for the advice to be prepared, and, in turn, to collect personal information contained in the advice. The Crown Solicitor has submitted that an agency could effectively be precluded from seeking professional advice, even where the advice merely repeats information that has been derived from the agency, because "[i]n many contexts, it is impracticable and often impossible to obtain the individual's authorisation for collection" from someone else.[8]

6.12 The Crown Solicitor has suggested that many of the problems associated with s 9 could be overcome by introducing an "unless

7. Crown Solicitor 's Office, New South Wales, *Advice*, [3.14].
8. Crown Solicitor 's Office, New South Wales, *Advice*, [3.14]. Although s 23(2) may permit collection in connection with court proceedings.

unreasonable or impracticable" rider to the s 9 requirement.[9] In addition, or alternatively, a provision could be introduced into PPIPA equivalent to s 7 of HRIPA. Section 7 of HRIPA provides that an individual is incapable of doing an act authorised, permitted or required by HRIPA if that individual is incapable, by reason of age, injury, illness or physical or mental impairment, of understanding the nature of the act or communicating his or her intentions with respect to the act.

6.13 UPP 2.3 of the UPPs proposed by the ALRC incorporates this test but as a leading phrase, rather than as a rider. UPP 2.3 states that: "If it is reasonable and practical to do so, an agency or organisation must collect personal information about an individual only from that individual."

6.14 However, further amendment of s 9 may still be needed to ensure that agencies can obtain external professional advice. Section 12(d) of PPIPA provides that, if it is necessary for an agency to give information that it holds to a person in connection with the provision of a service to the agency (such as providing financial or legal advice), it will do everything reasonably within its power to prevent unauthorised use or disclosure of that information. The Crown Solicitor has argued that "it is difficult to see how, as a matter of statutory construction, this impliedly authorises the disclosure and subsequent collection of personal information to and from the service provider".[10]

6.15 Privacy NSW is of the view that IPP 2 is too inflexible in the context of human services.[11] It has submitted that IPP 2 should be amended to allow indirect collection of personal information without the individual's authorisation where this is reasonably necessary in order to provide a service to a client. However, this should only be where indirect collection is solely for the purpose of, and necessary for, the provision of services, diagnosis, treatment or care to the client. Subsequent use and disclosure of the information should therefore be extremely limited.[12]

6.16 ***HPP 3:*** Unlike IPP 2, HPP 3 does not allow exceptions to the injunction to collect information directly from the individual. Even if an individual consents to third party collection, HPP 3 neither expressly nor impliedly permits this. The only exception to direct

---

9. See, for example, Health Privacy Principle 3(1): *Health Records and Information Privacy Act 2002* (NSW).
10. Crown Solicitor 's Office, New South Wales, *Advice*, [3.16].
11. Crown Solicitor 's Office, New South Wales, *Advice*, 44.
12. Crown Solicitor 's Office, New South Wales, *Advice*, 44.

collection of information from the individual concerned is if "it is unreasonable or impracticable to do so".

6.17 The Crown Solicitor is of the view that "the existence of consent" to collection of information would be a significant factor "to be taken into account in determining whether collection from an individual would be 'unreasonable'".[13] It is unclear what the Crown Solicitor means by "existence of consent". Whether or not there is consent can only be relevant where an individual refuses to provide, or withholds consent to collection of, personal information from him or herself, in which case the organisation may be able to rely on the "unreasonable or impracticable" exception to collect from a third party. An individual's consent to collection from a third party is irrelevant. The Commission is of the view that the approach of IPP 2 is to be preferred over that of HPP 3. We propose that, if there is to be one Act covering information privacy, IPP 2 be adopted, but if two separate Acts continue to operate, HPP should be amended to allow an individual to authorise collection by an organisation from a third party. We welcome submissions on our proposal.

PROPOSAL 8

If the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) are merged, the provision governing collection of personal information directly from an individual should contain the two exceptions currently provided for in IPP 2 together with a third exception currently provided for in HPP 3, namely that information must be collected from the individual unless it is "unreasonable or impractical to do so".

PROPOSAL 9

If two separate Acts continue to operate:

HPP 3 should be amended to allow an individual to authorise collection of his or her personal information by an organisation from someone else and to allow collection of information about an individual under 16 years from a parent or guardian; and

IPP 2 should be amended by introducing a further exemption, namely, that information must be collected from the individual unless it is "unreasonable or impractical to do so".

ISSUE 32

Should the *Privacy and Personal Information Protection Act 1998* (NSW) be amended by introducing a provision equivalent to s 7 of the *Health Records and Information Privacy Act 2002* (NSW) that an individual is incapable of doing an act authorised, permitted or required by the *Health Records and*

13. Crown Solicitor 's Office, New South Wales, *Advice*, [4.4].

Information Privacy Act 2002 **(NSW) if that individual is incapable, by reason of age, injury, illness or physical or mental impairment, of understanding the nature of the act or communicating his or her intentions with respect to the act?**

FURTHER COLLECTION REQUIREMENTS – IPP 3 AND IPP 4; HPP 4

6.18 IPP 3 (PPIPA s 10) provides that before information is collected from an individual, or as soon after as is practicable, the agency must make the individual to whom the information relates aware of a number of things. These include: the fact and the purpose of the collection; the intended recipients of the information; whether collection is required by law; rights to access and correct the information; and contact details of the collecting and holding agency (or agencies).

6.19 IPP 4 (PPIPA s 11) imposes further requirements on an agency for collection of information. It requires that the information be relevant to the purpose for which it is collected, not excessive, up to date and complete and that the collection does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

6.20 Privacy NSW has argued that s 10 is ambiguous in relation to whether the agency must notify the individual of the matters referred to in s 10, if the information was collected indirectly.[14] If, for example, the information was collected from a third party agency, Privacy NSW queries whether, in that case, the collecting agency must make the individual aware of these s 10 matters. Likewise, Privacy NSW has argued that s 11 does not make clear whether the requirements are equally applicable when information is collected from a third party as when it is collected directly from the individual.[15]

6.21 Around the time Privacy NSW issued its submission to the Attorney General's review of PPIPA, the ADT handed down a decision on the interpretation of s 10 and 11. In *HW v The Director of Public Prosecutions (No 2)*, the ADT held that s 10 and 11 only apply where an agency "collects personal information from an individual" to whom the information relates, not in relation to personal information from any individual.[16] The ADT stated that:

> [o]ne of the purposes of section 10 is to enable an individual to be fully informed of the relevant factors before deciding

14. Crown Solicitor 's Office, New South Wales, *Advice*, 45-46.
15. Crown Solicitor 's Office, New South Wales, *Advice*, 47.
16. *HW v The Director of Public Prosecutions (No 2)* [2004] NSWADT 73.

> whether to provide the information to the agency. This would not be a relevant consideration if the information is collected from a third party, and the individual to whom the information relates is separately informed of the collection.[17]

6.22 The Crown Solicitor has commented that it is unclear whether Parliament intended this distinction.[18] However, the Crown Solicitor argues that an expanded distinction would lead to practical difficulties (particularly where the information is collected in breach of s 9), such as where an agency was permitted under an exemption to s 9 to collect personal information from someone other than the individual. It has submitted that the status quo should be maintained.[19]

6.23 The Commission is not convinced that an individual should not have the opportunity of knowing: the fact that personal information about him or her has been collected from a third party; the purpose of the collection; the intended recipients of the information; whether collection is required by law; his or her rights to access and correct the information; and contact details of the collecting and holding agency (or agencies). We also question why an individual should not be protected by the requirements in s 11 just because the information has been collected from someone other than him or herself. This position is strengthened by the fact that the obligations imposed are not onerous. Each section carries the proviso that the agency need only "take such steps as are reasonable in the circumstances" to comply.

6.24 UPP 3.2 of the ALRC's proposed UPPs states that where collection is indirect, the agency or organisation must take reasonable steps to ensure that the individual is, or has been made aware of, the same matters as would have been conveyed if collection had been direct, as well as the source of the information, if requested by the individual.

6.25 HPP 4 takes a different, and clear, approach to making an individual aware of matters equivalent to the s 10 matters. It uses unequivocal wording in cl 4(1) that the subclause applies where an organisation "collects health information about an individual from the individual". Then, cl 4(2) applies to situations where "an organisation collects health information about an individual from someone else". It provides that the organisation must make the individual generally aware of the matters listed in subclause (1), except to the extent that this would pose a serious threat to the life or health of any individual; or the collection is exempted from compliance with subclause (2) by guidelines issued by the Privacy Commissioner.

---

17. *HW v The Director of Public Prosecutions (No 2)* [2004] NSWADT 73, [23].
18. Crown Solicitor 's Office, New South Wales, *Advice*, [3.17].
19. Crown Solicitor 's Office, New South Wales, *Advice*, [3.18].

PROPOSAL 10

IPPs 3 and 4 should be amended to stipulate that the requirements imposed by those sections apply whether the information is collected directly from the individual to whom the information relates or indirectly from someone else.

ISSUE 33

Should IPP 3 be amended to adopt the wording of HPP 4 or UPP 3.2, or some combination of the two?

APPLICATION OF IPPs TO RECORDS OF OBSERVATIONS OR CONVERSATIONS

6.26 A further issue with IPPs 3 and 4 raised by the Crown Solicitor relates to their application to records of observations or conversations. The Crown Solicitor has also pointed out a difficulty with IPP 9 (PPIPA s 16) in cases where the personal information has come from observations of, or conversations with, an individual and conclusions are drawn or opinions expressed based on those observations or conversations.[20]

6.27 *Vice-Chancellor, Macquarie University v FM* has established that personal information in the minds of employees is not "personal information held by" the agency.[21] Based on this authority, the Crown Solicitor has argued that the point at which information derived from observations or conversations is collected can only be the point at which it is recorded (such as in a file note). The Crown Solicitor is of the view that "[t]his arguably requires agencies to *then* comply with the notification requirements in s 10 and 11", but that "[t]his issue warrants clarification".[22]

6.28 With respect to IPP 9, there have been cases in the ADT where applicants have expected agencies to verify the accuracy of opinions or conclusions with them, which, the Crown Solicitor has argued, "effectively makes the external review provisions of PPIPA a quasi-defamation proceeding".[23] The Crown Solicitor has commented that the proviso in s 16 (also present in HPP 9) that the agency need only take "such steps as are reasonable in the circumstances" may act as a sufficient safeguard. Nonetheless, the Crown Solicitor has submitted that, as with s 10 and 11, the application of s 16 to personal

20. Crown Solicitor 's Office, New South Wales, *Advice*, [3.23].
21. *Vice-Chancellor, Macquarie University v FM* [2005] NSWCA 192.
22. Crown Solicitor 's Office, New South Wales, *Advice*, [3.19].
23. Crown Solicitor 's Office, New South Wales, *Advice*, [3.23].

information that has come from observations of, or conversations with, an individual would benefit from clarification.[24]

PROPOSAL 11

IPPs 3 and 4 should be amended to clarify that the word "collects" means, in relation to information derived from observations of, or conversations with, an individual, the point at which information is recorded.

ISSUE 34

Should IPP 9 and HPP 9 apply to personal information that consists of conclusions drawn, or opinions expressed, based on observations of, or conversations with, an individual, providing a record is made of those conclusions or opinions? If so, do these provisions require amendment to clarify this?

RETENTION AND SECURITY OF INFORMATION – IPP 5; HPP 5

6.29 IPP 5 (PPIPA s 12) and HPP 5 require an agency/organisation to ensure that information is: held for no longer than necessary; disposed of securely; and protected against loss and unauthorised access, use, modification or disclosure. In addition, if it is necessary to give the information to a service provider, the agency/organisation must do everything reasonably within its power to prevent unauthorised use or disclosure.

6.30 Privacy NSW has made the point that missing from the requirements imposed by IPP 5 and HPP 5 is the requirement for secure collection of information.[25] This is particularly relevant in the electronic age when information is frequently collected by email and from the internet. There are no obligations imposed by IPP 5 and HPP 5 for an agency to provide a secure website or email address and to limit access to these collection points by others. While the question of secure disposal of hard drives (on which material is retained even if the user deletes the file) and access to back-up tapes is relevant to storage of information, it is also relevant to providing secure collection.

PROPOSAL 12

IPP 5 and HPP 5 should be amended to include a requirement for the secure collection of personal information.

24. Crown Solicitor 's Office, New South Wales, *Advice*, [3.23].
25. Crown Solicitor 's Office, New South Wales, *Advice*, 48.

ACCESS TO, AND ALTERATION OF, INFORMATION – IPP 7 AND IPP 8; HPP 8

6.31 IPP 7 (PPIPA s 14) gives an individual a right to access his or her personal information, and IPP 8 (PPIPA s 15) and HPP 9 give the individual a right to request amendments to ensure that the information is accurate, relevant to the purpose of collection, up to date, complete and not misleading.

6.32 Privacy NSW has submitted, in relation to PPIPA, that the usefulness of s 14 and 15 is diminished by s 20(5) due to a "lack of clarity about the breadth of [their] application".[26] The lack of clarity lies with s 20(5) of PPIPA rather than with s 14 and 15 themselves. Section 20(5) of PPIPA and s 22(3) of HRIPA are equivalent provisions. To make for easier reading, the following discussion focuses on s 20(5) of PPIPA but the comments apply equally to s 22(3) of HRIPA, as does Privacy NSW's criticism of the interaction between s 20(5) and s 14 and 15. Section 22(3) of HRIPA applies to HPPs 6, 7 and 8, which correspond to IPPs 6, 7 and 8 (s 13, 14 and 15 of PPIPA).

6.33 Section 20(5) provides that the provisions of the *Freedom of Information Act 1989* (NSW) ("FOI Act") that impose conditions or limitations on any matter referred to in IPPs 6, 7 or 8 are not affected by PPIPA and the FOI Act provisions continue to apply as if part of PPIPA. The difficulty with s 20(5) is the uncertainty, and lack of guidance, as to what are "conditions" or "limitations" in the FOI Act.[27]

6.34 Privacy NSW has argued that it is uncertain exactly how "the access and correction provisions of the FOI Act relate to or are imported into" PPIPA.[28] It queries, as examples of this uncertainty, whether s 20(5) has the effect of importing into PPIPA from the FOI Act: the requirement to lodge a request in writing, or to pay prescribed fees; the Schedule 1 list of exempt documents; the Schedule 2 list of exempt bodies; or the consultation requirements in Part 3.[29] Privacy NSW concludes that the benefits of the less formal approach to request access to, or amendment of, one's own personal information in

---

26. Crown Solicitor 's Office, New South Wales, *Advice*, 50.
27. Crown Solicitor 's Office, New South Wales, *Advice*, 82. The Crown Solicitor, commenting that s 20(5) is "not an easy provision to construe", has observed that "[t]he difficulty lies in identifying the provisions of the FOI Act that impose 'conditions or limitations (however expressed)' with respect to any 'matter' referred to in ss 13, 14 or 15": Crown Solicitor 's Office, New South Wales, *Advice*, [7.1].
28. Crown Solicitor 's Office, New South Wales, *Advice*, 82.
29. Crown Solicitor 's Office, New South Wales, *Advice*, 82.

IPPs 7 and 8 are lost "if the request must in effect become an FOI application".[30]

6.35 Privacy NSW has further pointed out that the FOI Act only applies to "documents" and it is unclear how this affects, by reason of s 20(5), the much broader definition of "information" under PPIPA.[31] The operation of IPP 8 in particular is made unclear by the application of s 20(5) because the FOI Act does not provide for the deletion of "information". How does this affect the requirement in IPP 8 to delete personal information where appropriate?

PROPOSAL 13

The meaning and effect of s 20(5) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 22(3) of the *Health Records and Information Privacy Act 2002* (NSW), and their application to the IPPs and HPPs respectively, should be clarified.

6.36 A further issue arises specifically in relation to s 15 of PPIPA because of an apparent inconsistency between sub-sections (1) and (2).[32] Section 15(1) provides that an agency *must* amend personal information if requested, whereas s 15(2) provides that, if the agency is *not prepared* to make the amendments as requested then certain steps follow. The ADT has been reluctant to read down s 15(1) so as to hold that the only amendments that can be made under that sub-section are notations made in accordance with s 15(2).[33]

6.37 Both the Crown Solicitor and the Ombudsman make the point that although s 15(1) provides that an agency "must" make appropriate amendments, s 15(2) suggests that the agency may choose not to make the requested amendments.[34] Possibly, the use of the word "ensure" in s 15(1) (the agency must amend information "to ensure" its accuracy etc) means that an agency is only under an obligation to make amendments if it can "ensure" the matters set out in s 15(1)(a) and (b). However, if this is the correct interpretation, PPIPA provides no guidance on the level of proof required to meet the "ensure" requirement.

6.38 The Ombudsman has suggested that the effect of the section is that it requires a threshold test: first, the agency must determine whether or not the personal information is accurate, relevant, up-to-date, complete and not misleading; if not, the information *must* be

---

30. Crown Solicitor 's Office, New South Wales, *Advice*, 83.
31. Crown Solicitor 's Office, New South Wales, *Advice*, 83.
32. The Crown Solicitor has stated that the effect of s 15(1) and (2) is unclear: Crown Solicitor 's Office, New South Wales, *Advice*, [3.20].
33. See *GR v Department of Housing* [2003] NSWADT 268, [41].
34. Crown Solicitor 's Office, New South Wales, *Advice*, [3.20].

amended. Section 15(2) should then only relate to the situation where the information is accurate, relevant, up-to-date, complete and not misleading but the individual still asks for an amendment.

6.39 Two ways of clarifying the operation of s 15 have been suggested. First, “must” in s 15(1) can be construed as “may”. The Commission does not favour this approach as the statutory construction is clear. Further, it is proper that an individual have the right to correct his or her personal information. Why should inaccurate, irrelevant, out-of-date, incomplete or misleading information be allowed to remain in the agency’s possession and control? Alternatively, s 15(2) could be amended to provide: “if a public sector agency is not required to amend personal information under s 15(1)(a) and believes on reasonable grounds that it has complied with s 15(1)(b), the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such manner as is capable of being read with the information, any statement provided by that individual of the amendment sought”.

ISSUE 35

Does the effect of s 15(1) and (2) of the *Privacy and Personal Information Protection Act 1998* (NSW) need clarification? If so, how should one or both sections be amended to reconcile their operation?

THE DICHOTOMY BETWEEN “USE” AND “DISCLOSURE” – IPPs 9, 10, 11 AND 12; HPPs 9, 10, 11 AND 12

6.40 IPP 9 (PPIPA s 16) and HPP 9 require an agency/organisation to take reasonable steps to check that information is relevant, accurate, up to date, complete and not misleading before it uses the information. IPP 10 (PPIPA s 17) and HPP 10 limit an agency’s use of personal information, but not disclosure. Limits on disclosure are separately dealt with in IPPs 11 and 12 (PPIPA s 18 and 19), the latter focusing on disclosure of sensitive information, and in HPP 11.

6.41 Although HRIPA separates “use “ and “disclosure” in HPP 10 and HPP 11, the grounds in HPP 10 for allowing “use” are repeated in HPP for allowing “disclosure”. The only difference between the two provisions is that HPP 11 adds a further exception in HPP 11(g) of “compassionate reasons”.

6.42 Privacy NSW points out that this dichotomy between “use” and “disclosure” is largely a peculiarity of Australasian privacy legislation and that in other jurisdictions use and disclosure are dealt with

together, often under a generic expression like "processing".[35] It is interesting to note that the original OECD Guidelines covered both concepts within the one "Use Limitation" principle, which applied to information "disclosed, made available or otherwise used".[36] Privacy NSW also explains that separating the concepts of "use" and "disclosure" has its historical roots in the original privacy principles in the Commonwealth *Privacy Act*. However, history has overtaken this legislative approach. The distinction has been removed in more recently drafted privacy laws such as the National Privacy Principles for the private sector inserted into the *Privacy Act 1988* (Cth) in 2000.[37] The UPPs proposed by the ALRC, although not adopting a single word to encompass use and disclosure, deal with "use and disclosure" together in one UPP, namely UPP 5.

6.43 Any argument that rules of statutory interpretation would suggest that the references to "use" and "disclosure" should be construed as having the same meaning, has been rejected by the ADT. In *NZ v Director General, New South Wales Department of Housing*, the ADT held that "use" refers to "the handling of personal information within the collecting agency" and "disclosure" to "the giving of the information by the collecting agency to a person or body outside the agency".[38] Similarly, in *JD v Department of Health*, the Appeal Panel held that "'use' normally bears the connotation of employing information for a purpose" and if an agency "merely retrieves information in its possession and discloses that to an external person or body, there is no 'use' involved".[39]

6.44 However, the Crown Solicitor has suggested that the distinction between "use" and "disclosure" is not as clear-cut as the ADT has assumed.[40] The issue is complicated by s 28(3) because it implies that s 17 deals with "disclosure".[41] In addition, the distinction between "use" and "disclosure" has been blurred in relation to s 16 by the conclusion in *Director General, Department of Education and Training v MT* that s 16 "applies a data quality standard to all uses of personal

---

35. Crown Solicitor 's Office, New South Wales, *Advice*, 52. See, for example, the *Personal Information Protection and Electronic Documents Act 2000* (Canada), sch 1, Principle 5; the *Data Protection Act 1998* (UK) sch 1, Data Protection Principle 6.
36. Pointed out by Crown Solicitor 's Office, New South Wales, *Advice*, 52.
37. See also the *Information Privacy Act 2002* (Vic).
38. *NZ v Director General, New South Wales Department of Housing* [2005] NSWADT 58, [69].
39. *JD v Department of Health* [2005] NSWADTAP 44, [93], [42].
40. Crown Solicitor 's Office, New South Wales, *Advice*, [3.41].
41. Crown Solicitor 's Office, New South Wales, *Advice*, [3.41]. Section 28(3) of *Privacy and Personal Information Protection Act 1998* (NSW) provides that "nothing in section 17, 18 or 19 prevents or restricts the disclosure of information ..."

information by an agency including conduct involving disclosure of personal information by the agency".[42]

6.45 Privacy NSW argues that having different IPPs apply to use and disclosure is untenable for two reasons. First, it gives rise to technical arguments as to when processing of information involves use or disclosure. Secondly, it involves an unjustifiable application of different standards.[43] For example, IPP 12 gives sensitive information a higher degree of protection with respect to disclosure than it receives with respect to use. Specifically in relation to s 16, the Commission is of the view that logically, and in fairness to the individual to whom the information relates, the provision should place an agency/organisation under the same obligation to check information before disclosing it as applies to use of the information.

6.46 Privacy NSW has recommended either collapsing the concepts of "use" and "disclosure" into one concept or matching exactly the privacy standards, and exemptions from those standards, for "use" and "disclosure" contained in the HPPs.[44]

ISSUE 36

(a) Should "use" and "disclosure" be treated as one concept such as "processing", or as a combined phrase such as in the proposed UPP 5, with the one set of privacy standards and exemptions applying?

(b) Alternatively, should the same privacy standards, and exemptions from those standards, contained in the HPPs apply equally to "use" and "disclosure" of information?

IDENTIFICATION OF THE PURPOSE FOR COLLECTION – IPPs 10 AND 11; HPPs 10 AND 11

6.47 Although IPPs 10 and 11 (PPIPA s 17 and 18) and HPPs 10 and 11 regulate separate matters ("use" in 10; "disclosure" in 11), these privacy principles all limit the agency's/organisation's use or disclosure of the information to a purpose "for which it was collected".[45] Note that the wording is not "for which the agency/organisation collected it" or similar.

---

42. *Director General, Department of Education and Training v MT* [2005] NSWADTAP 77, [39].
43. Crown Solicitor 's Office, New South Wales, *Advice*, 53.
44. Crown Solicitor 's Office, New South Wales, *Advice*, Recommendation, 53.
45. The phrase used in s 11 of *Privacy and Personal Information Protection Act 1998* (NSW) is "for which the information was collected".

6.48 The Crown Solicitor has argued that these provisions fail to recognise that there may be multiple lawful acts of collection, such as where an agency is entitled to collect information from someone other than the individual pursuant to the exemptions in s 9 of PPIPA.[46] The purpose for which the individual gave his or her personal information to a third party may be quite different from the purpose for which an agency collects that information from the third party.

ISSUE 37

Is the correct interpretation of IPPs 10 and 11 and HPPs 10 and 11 that the relevant purpose is the one for which the agency/organisation collected it? If so, should the provisions be amended to clarify this?

APPLICATION OF IPPs 10 AND 11 AND HPPs 10 AND 11 TO UNSOLICITED INFORMATION

6.49 Section 4(5) of PPIPA and s 10 of HRIPA provide that personal information is not "collected" if receipt of the information by the agency/organisation is unsolicited. Accordingly, the collection IPPs 1-4 (PPIPA s 8-11) and HPPs 1-4 do not apply to unsolicited information. The question that arises is, if IPPs 10 and 11 and HPPs 10 and 11 depend on identification of the purpose for which information was "collected", how can these provisions be applied where there is no "collection"?

6.50 In *KD v Registrar, New South Wales Medical Board*, the ADT held that s 17 and 18(1) of PPIPA can have no application where the information is unsolicited.[47] However, in *OA v New South Wales Department of Housing*, the ADT held that "the principles in the Act that have to do with 'holding' of information come into play; as do the principles in relation to 'use' and 'disclosure' [where an agency] decides to 'hold' information that was originally received as an unsolicited communication".[48] The ADT considered that "collection" occurred "when the Department decided to retain the unsolicited information and keep it essentially as intelligence information".[49] The deemed purpose of collection is, in effect, the purpose for which it was retained. The Crown Solicitor questions whether this approach is correct.[50] It argues that, taken to its logical conclusion, if a "collection" occurs when the agency decides to keep the information, then all the collection IPPs (and, by extension, HPPs), including s 9, should apply.

---

46. Crown Solicitor 's Office, New South Wales, *Advice*, [3.24-3.32].
47. *KD v Registrar, New South Wales Medical Board* [2004] NSWADT 5.
48. *OA v New South Wales Department of Housing* [2005] NSWADT 233, [45].
49. *OA v New South Wales Department of Housing* [2005] NSWADT 233, [50].
50. Crown Solicitor 's Office, New South Wales, *Advice*, [3.28].

6.51 In *AW v Vice Chancellor, University of Newcastle*, the ADT held that IPP 10 and HPP 10 applied to unsolicited information.[51] Health and other information was provided by the applicant to the University to support his complaint to the University that he was suffering harassment and discrimination at the hands of students and lecturers. The applicant applied to the ADT for review of conduct whereby his information was, he alleged, disclosed by the University to others in breach of the IPPs and HPPs. The ADT found that the information was unsolicited and that the "collection" IPPs and HPPs did not therefore apply.[52] However, the ADT then went on to hold that the information was "held" by the University and that the "use" privacy principles (IPP 10; HPP 10) accordingly applied.[53] While the ADT found that the information was unsolicited and hence not "collected" by virtue of s 4(5) of PPIPA and s 10 of HRIPA, it found that the meaning of "collected" in the context of IPP 10 and HPP 10 was wider. That is, IPP 10 and HPP 10 state that an agency/organisation must not use information for a purpose other than that for which it was collected but in this context, "collected" could mean "obtained".[54]

6.52 The approach taken by the ALRC in its proposed UPP 2.5 is to provide that, if an agency or organisation receives unsolicited personal information, it must either: destroy it without using or disclosing it; or comply with all relevant UPPs as if the agency/organisation had actively collected the information.

ISSUE 38

Do IPPs 10 and 11 and HPPs 10 and 11 apply to unsolicited information? If not, should they apply?

ISSUE 39

Should the privacy principles include a principle in terms identical, or equivalent, to the proposed UPP 2.5?

DISCLOSURE TO THIRD PARTIES – IPP 11

6.53 IPP 11, specifically s 18(1)(b) of PPIPA, exempts from the requirement not to disclose information to a third party the situation where the individual to whom the information relates "is reasonably

51. *AW v Vice Chancellor, University of Newcastle* [2008] NSWADT 86.
52. *AW v Vice Chancellor, University of Newcastle* [2008] NSWADT 86, [27].
53. *AW v Vice Chancellor, University of Newcastle* [2008] NSWADT 86, [28]. The ADT ultimately found that the evidence did not disclose any breach of the "use" privacy principles: [30].
54. *AW v Vice Chancellor, University of Newcastle* [2008] NSWADT 86, [28], relying on *MT v Department of Education and Training* [2004] NSWADT 194.

likely to have been aware, or has been made aware in accordance with s 10, that information of that kind is usually disclosed" to that third party.

6.54 The Crown Solicitor has pointed out that missing from this sub-section is the wording in s 18(1)(a) "and the agency … has no reason to believe that the individual concerned would object to the disclosure".[55] Hence, under s 18(1)(b), even if the individual objects, an agency could still lawfully disclose information if the other prerequisites are met. This may be acceptable if the individual is aware, or made aware, before providing the information that it may be disclosed to a third party. However, if the individual is in fact not aware, and given that s 10 allows the agency to inform the individual "as soon as practicable after collection" and that s 18 contains no mechanism to retract the information, it is arguable that the provision operates unfairly.

6.55 Proposed UPP 3.1(f) does not remedy the problem as it too allows an agency or organisation to inform an individual of the "types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information" *after* collection (albeit as soon as practicable after collection).[56]

ISSUE 40

(a) Should s 18(1)(b) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to include the phrase "and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure"?

(b) Alternatively, should s 18(1)(b) be amended to delete the reference to s 10 and to provide instead that the individual must be made aware at the time the information is collected that information of that kind is usually disclosed to a third party?

SPECIAL RESTRICTIONS ON DISCLOSURE – IPP 12

Section 19(1) of PPIPA – disclosure of sensitive information

6.56 As noted above, s 19(1) applies restrictions to the disclosure of "personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities", which can be loosely termed

55. Crown Solicitor 's Office, New South Wales, *Advice*, [3.29].
56. UPP 3.2 applies the provisions of UPP 3.1 to information collected from someone other than the individual.

"sensitive information". A higher standard must be met before sensitive information can be disclosed.

6.57 Privacy NSW has submitted that a person's criminal history or record should be included in the types of sensitive information covered by s 19(1).[57] This is the approach taken in the *Privacy Act 1988* (Cth),[58] the *Information Privacy Act 2000* (Vic)[59] and the *Information Act* (NT).[60] Privacy NSW reports that about six per cent of the complaints and enquiries it receives relate to misuse of a person's criminal history or record and that "[i]nappropriate disclosure of spent convictions is of particular concern, especially in the employment context".[61]

6.58 The statutory review of PPIPA observed that "the legislation in NSW governing criminal records deals only with spent convictions" and that "[i]t is appropriate for privacy legislation to protect personal information concerning a person's criminal record if it is not otherwise protected".[62] The review recommended that "the definition of sensitive personal information in the Act … include a person's criminal record".[63]

6.59 Privacy NSW has also submitted that the words "sexual activities" in s 19(1) need clarification, as it is unclear whether the reference is to sexual orientation or sexual conduct (for example, adultery, sexual assault, sexual harassment), or both.

6.60 Privacy NSW has further submitted that the structure of s 18 and 19 could be improved. It suggests that the separation of s 19(1) from s 18 has caused confusion and that there have been instances where the stricter requirements for disclosure of sensitive information have been overlooked. Given that the remainder of s 19 deals with trans-border information disclosure, Privacy NSW has suggested that s 19(1) would more logically fit into s 18.

ISSUE 41

Should disclosure of an individual's criminal history and record be restricted under s 19 of the *Privacy and Personal Information Protection Act 1998* (NSW)?

57. Crown Solicitor 's Office, New South Wales, *Advice*, 57.
58. See National Privacy Principles 2 and 10.
59. See IPP 10.
60. See IPP 10.
61. Crown Solicitor 's Office, New South Wales, *Advice*, 57.
62. New South Wales Attorney General's Department, *Review of Privacy and Personal Information Protection Act 1998* (NSW) (tabled 25 September 2007, Legislative Assembly),[9.44].
63. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998* (NSW), Recommendation 17.

ISSUE 42

Should the meaning of the words "sexual activities" in s 19(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) be clarified?

ISSUE 43

Should s 19(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) be taken out of s 19 and placed within s 18?

Section 19(2) of PPIPA – disclosure outside NSW

6.61 Section 19(2) of PPIPA prohibits the disclosure of information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency, unless a relevant privacy law applying to that information is in force in that jurisdiction, or applies to that Commonwealth agency; or the disclosure is permitted under a privacy code of practice. Section 19(4) provides that the Privacy Commissioner "is to prepare a code relating to disclosure of personal information" to external jurisdictions or Commonwealth agencies.

6.62 If, as seems likely, s 19(2) is the sole provision relating to disclosure of information outside New South Wales, and s 18(1) is not also applicable, then both the Crown Solicitor and the Privacy Commissioner have said that s 19(2) will not apply until a code referred to in s 19(4) has been made.[64] If this interpretation is correct there are presently no limitations on the disclosure of personal information to interstate bodies and Commonwealth agencies as no such code has been made to date.

6.63 HPP 14 regulates the "transfer" of "transborder data flows and "data flow to Commonwealth agencies". Transfer of health information to external jurisdictions or Commonwealth agencies is not permitted unless one of eight criteria is satisfied. Either:

(a) the organisation reasonably believes that the recipient of the information is subject to principles for fair handling of the information that are substantially similar to the HPPs;

(b) the individual consents;

(c) and (d) the transfer is necessary to perform a contract either between the individual and the organisation, or between the organisation and a third party in the individual's interest, or to implement pre-contractual measures at the individual's request;

---

64. Crown Solicitor 's Office, New South Wales, *Advice*, [3.36]; NSW Privacy, *Consultation* (29 June 2007).

(e) the transfer is for the individual's benefit, it is impracticable to obtain his or her consent and he or she would be likely to consent anyway;

(f) the organisation reasonably believes the transfer to be necessary to lessen or prevent a serious and imminent threat to life, health or safety, or serious threat to public health or safety;

(g) the organisation has taken reasonable steps to ensure the information will be treated consistently with the HPPs; or

(h) the transfer is permitted or required by law.

The operation of the provision is not dependent on a health privacy code of practice being made.

6.64 Proposed UPP 11 similarly regulates transborder data flows to jurisdictions outside Australia by making the transfer conditional upon (at least) one of four circumstances prevailing. Two of these are similar to criteria (a) and (b) of HPP 14 and two differ: (a) the agency or organisation reasonably believes that the recipient of the information is subject to principles for fair handling of the information that are substantially similar to the UPPs; or (b) the individual consents; or (c) the transfer is necessary for an enforcement body to carry out certain enforcement roles; or (d) the agency or organisation continues to be liable for breaches of the UPPs and certain other conditions are met.

6.65 The Commission considers that HPP 14 and UPP 11 are far better provisions to regulate transborder data flow and transfer of information to Commonwealth agencies than s 19(2) of PPIPA, but we are interested to receive responses to our provisional view.

PROPOSAL 14

Section 19(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be redrafted in line with HPP 9 and the proposed UPP 11. Alternatively, if the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) are to become one Act, HPP 9, redrafted to incorporate elements of the proposed UPP 11, is to be preferred over s 19(2) to regulate transborder data flows and transfer of information to Commonwealth agencies.

REGULATING UNIQUE IDENTIFIERS

6.66 An "identifier" is usually, but not necessarily, a number (although, it cannot simply be the individual's name) assigned to an individual by an agency for the purpose of uniquely identifying that individual.[65]

6.67 Legislation that regulates identifiers generally does so by providing that an agency/organisation may only assign an identifier to an individual if this is reasonably necessary to carry out its functions efficiently. Also, generally speaking, "identifier" provisions ensure "single purpose use" of identifiers. That is, a private sector person can only adopt as its own identifier of an individual, or use or disclose, an identifier that a public sector agency has assigned to that individual in specific situations. These include where: the individual consents; adopting the identifier is required or authorised by law; or the use or disclosure is required for the purpose the identifier was assigned.[66] There are also exceptions to the rule that a private sector person cannot adopt, use or disclose an identifier assigned by a public sector agency in situations where this is necessary for the private sector person to fulfil its obligations to, or the requirements of, the public sector agency.[67]

6.68 Of all privacy statutes in Australian jurisdictions, including the Commonwealth, PPIPA is the only one that does not include a provision regulating the use of unique identifiers.[68] In the Commission's view, this is an omission that needs to be rectified.

---

65. See, for example, the definition of "identifiers" in s 4 of the *Health Records and Information Privacy Act 2002* (NSW).
66. See, for example, *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 12(2) and (3).
67. See, for example, *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 12(4).
68. See the *Privacy Act 1988* (Cth), sch 3 cl 7 (National Privacy Principle 7); *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 12 (HPP 12); *Personal Information Protection Act 2004* (Tas) s 24; *Information Act* (NT), sch 2; *Information Privacy Act 2002* (Vic) s 7.

6.69 The danger of an agency disclosing its unique identifier for an individual to other bodies or organisations, other than in restricted circumstances, is that the third party may be able to access information about the individual connected with the unique identifier for unauthorised purposes. There is a belief that threats to privacy are inherent in any unique identifier for individuals. Use of the same identifier by different organisations "increases the threat to privacy by facilitating unauthorized linkages of information about an individual within and across those organizations",[69] particularly in an electronic environment. If a social security number, for example, were to be used as a unique identifier, this could allow access to a large amount of very private information, such as medical, credit and financial data, consumer behaviour information and employment information.

6.70 Individuals whose personal information comes within the jurisdiction of PPIPA are in a vulnerable position in the absence of a provision regulating use and disclosure of identifiers. Furthermore, PPIPA is out of step with other jurisdictions. PPIPA should be amended to include, or a remodelled PPIPA/HRIPA Act should contain, a provision regulating identifiers. Whether the provisions of HPP 12 or the proposed UPP 10, or some combination of the two, should be adopted is a matter for consultation.

6.71 The proposed UPP 10 and HPP 12 are quite different. UPP 10 omits the provision contained in HPP 12(1) permitting an agency to assign an identifier if this is reasonably necessary to carry out its functions efficiently. UPP 10 is focused solely on ensuring "single use" of identifiers by stating that an organisation or an agency must not adopt as its own an identifier that has been assigned by another agency (including a State or Territory agency), an agent or a contractor. HPP 12(2), however, allows a private sector person to adopt as its own an identifier assigned by a public sector agency (or agent or contractor) if: the individual consents to the adoption of the same identifier; or the use or disclosure of the identifier is required or authorised by or under law. Pursuant to UPP 10.4, an agency or organisation identifier must not be disclosed by an agency or organisation unless the use or disclosure: (a) is necessary for the agency or organisation to fulfil its obligations to the agency that assigned the identifier; or (b) is subject to one or more of the use and disclosure UPPs (UPP 5.1(c) to (f)); or (c) would be permitted by the proposed Privacy (Health Information) Regulations where the identifier is genetic information; or (d) is of a prescribed identifier in

---

69. U.S. Department of Health and Human Services, *Unique Health Identifier for Individuals: A White Paper* (1998) http://www.epic.org/privacy/medical/hhs-id-798.html (27 November 2007).

prescribed circumstances. HPP 12(3), on the other hand, allows use or disclosure by a private sector person of an identifier assigned by a public sector agency (or agent or contractor) if the use or disclosure: (a) is required for the purpose for which it was assigned, or a described secondary purpose; or (b) is consented to by the individual; or (c) is disclosure back to the assigning agency to enable the agency to identify the individual for its own purposes.

PROPOSAL 15

If the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) are to become one Act, a privacy principle regulating the use and disclosure of identifiers should be contained in the new Act. If the two Acts are to remain separate, the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended by the addition of a further IPP regulating the use and disclosure of identifiers.

ISSUE 44

Should the privacy principle regulating the use and disclosure of identifiers be in the same terms as HPP 12 or the proposed UPP 10, or some combination of the two?

7. Other operational issues

- Introduction
- Exemptions
- Privacy codes of practice - PPIPA Part 3; HRIPA Part 5
- The meaning of “person” in s 37 and 38 of PPIPA
- Public interest directions - PPIPA s 41 ; HRIPA s 62
- Complaints under s 45 of PPIPA
- Review of conduct by the ADT - PPIPA Part 5; HRIPA s 21

INTRODUCTION

7.1 This chapter continues the examination, begun in Chapter 6, of problems, uncertainties and ambiguities with the operation of the *Privacy and Personal Information Protection Act 1998* (NSW) ("PPIPA") and the *Health Records and Information Privacy Act 2002* (NSW) ("HRIPA").

7.2 Whereas Chapter 6 was confined to assessing the Information Protection Principles ("IPPs") and the Health Privacy Principles ("HPPs"), this chapter deals with a number of diverse issues, including:

- a dichotomy in the operation of exemptions from the IPPs where an agency is investigating a complaint;
- uncertainty in the operation of exemptions from the IPPs where non-compliance is permitted or required under an Act or any other law;
- ambiguity in the scope of privacy codes of practice;
- uncertainty and inconsistency in the meaning of the word "person" in Part 4 of PPIPA, particularly in s 37 and 38;
- a drawback with the operation of the public interest directions provisions;
- issues arising in relation to making a complaint including: who may make a complaint; criteria to be applied by the Privacy Commissioner; how s 45 and 36(2)(k) of PPIPA operate together; the application of s 51 of PPIPA to withdrawn complaints; and uncertainty with the operation of s 65 of PPIPA, which deals with reports to Parliament; and
- issues arising in relation to review of conduct by the Administrative Decisions Tribunal ("ADT") including: the nature of the ADT's jurisdiction; the absence of a limitation period for review by the ADT; the ADT's powers on review; the role of the Privacy Commissioner in appeals from ADT decisions; and whether final determination of complaints should be made by the ADT or the Privacy Commissioner.

EXEMPTIONS

Section 24 of PPIPA – exemptions relating to investigative agencies

7.3 The exemptions from compliance with IPPs 2, 3, 10 and 11 (PPIPA s 9, 10, 17 and 18) contained in s 24 apply to an agency that is itself investigating a complaint.[1] The exemptions do not, however, apply when an agency is disclosing personal information to an investigative agency for the purpose of that investigative agency carrying out its complaints-handling or investigative functions.

7.4 This seems to the Commission to be a dichotomy that is difficult to justify. It also creates problems for agencies that do not have coercive powers, or in situations where coercive powers are not available.[2] While the issue has been addressed in a direction made by the Privacy Commissioner pursuant to s 41, entitled "The use of information for investigative purposes", we query whether it should be addressed in legislation.

ISSUE 45

Should s 24 of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to exempt an agency from compliance with IPPs 2, 3, 10 and 11 when the agency is disclosing personal information to an investigative agency for the purpose of that investigative agency carrying out its complaint handling or investigative functions?

Section 25 of PPIPA – exemptions where non-compliance is otherwise permitted

7.5 Pursuant to s 25 of PPIPA, an agency is not required to comply with IPPs 2, 3, 6, 7, 8, 10, 11 and 12 (PPIPA s 9, 10, 13, 14, 15, 17 18 and 19)[3] if (a) it is "lawfully authorised or required not to comply"; or (b) "non-compliance is otherwise permitted … under an Act or any other law".

1. *Privacy and Personal Information Protection Act 1998* (NSW) s 24(4): "The exemptions … extend to any public sector agency … who is 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."
2. See Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.44].
3. See HPPs 4(4), 5(2), 6(2), 7(2), 8(4), 10(2), 11(2) and 15(2).

7.6 The Crown Solicitor suggests that it is not clear whether exemption (a) should be limited to cases where a statutory provision expressly refers to the relevant IPP and provides that an agency is authorised or required not to comply with it.[4]

7.7 While this limited interpretation of s 25(a) is defensible, in *HW v Commissioner of Police, New South Wales Police Service*, the ADT took a broader view, holding that disclosure of documents to the District Court by the DPP was done "lawfully and in accordance with the duty to the court" because the disclosure was pursuant to a subpoena. In those circumstances, s 25(a) was held to apply.[5]

ISSUE 46

(a) Is the correct interpretation of s 25(a) of the *Privacy and Personal Information Protection Act 1998* (NSW) that it applies to cases where a statutory provision expressly refers to the relevant IPP and provides that an agency is authorised or required not to comply with it, or is a wider interpretation correct, such as adopted by the Administrative Decisions Tribunal in *HW v Commissioner of Police, New South Wales Police Service*?

(b) Should s 25(a) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to clarify its application?

7.8 The reference in s 25(b) to "any other law" has been held by the Appeal Panel of the ADT to include the common law.[6] The Crown Solicitor has suggested that this would be made clearer by re-ordering the words in that subsection, so that the words in parenthesis "(including the *State Records Act 1998*)" followed the words "under an Act".[7] The Commission agrees that this would remove any doubt that "any other law" is restricted to legislative instruments. It is also a simple, non-controversial, amendment to make.

4. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.45].
5. *HW v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 214, [64].
6. *Director General, Department of Education and Training v MT* [2005] NSWADTAP 77, [84]. See also *KD v Registrar, New South Wales Medical Board* [2004] NSWADT 5, [34]; and *HW v Commissioner of Police* [2003] NSWADT 214.
7. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.47].

PROPOSAL 16

Section 25(b) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to read as follows:
"A public sector agency is not required to comply with section 9, 10, 13, 14, 15, 17 18 or 19 if:
...
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act (including the *State Records Act 1998*) or any other law."

Application of s 25(b) to a preliminary inquiry by the Ombudsman

7.9 An issue arises as to whether disclosure of personal information by an agency in response to a preliminary inquiry made by the Ombudsman pursuant to s 13AA of the *Ombudsman Act 1974* (NSW) attracts the exemption of s 25(b) of PPIPA.[8] If it does not, the disclosure must comply with the restrictions imposed by IPP 11 (PPIPA s 18).

7.10 The Ombudsman has been advised that s 25(b) does not apply to a preliminary inquiry and has interpreted this to mean that agencies are prevented from disclosing "personal information" to the Ombudsman, or any other complaints-handling body, in response to informal or preliminary inquiries.[9] The Ombudsman points out that it deals with most complaints within its general and community services jurisdictions by conducting preliminary inquiries to decide whether to conduct a formal investigation into the conduct about which there has been a complaint. It submits that the need to comply with s 18 would have significant implications for the ability of complaints-handling bodies to resolve matters informally or for those bodies who have limited statutory powers to require answers to questions.[10]

7.11 The Ombudsman has suggested that this could be remedied by excluding public sector agencies from compliance with s 18 if the information is disclosed to an investigative agency in order that it may exercise its complaints-handling or investigative functions.[11]

---

8. Section 13AA(1) of the *Ombudsman Act 1974* (NSW) provides: "The Ombudsman may make preliminary inquiries for the purpose of deciding whether to make particular conduct of a public authority the subject of an investigation under this Act.
9. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (April 2004), 26.
10. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998*, 26.
11. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998*, 26.

ISSUE 47

Should public sector agencies be exempted from compliance with s 18 of the *Privacy and Personal Information Protection Act 1998* (NSW) if the information is disclosed to an investigative agency in order that it may exercise its complaints-handling or investigative functions?

PRIVACY CODES OF PRACTICE - PPIPA PART 3; HRIPA PART 5

7.12 The precise scope of codes of practice may need clarifying. Section 29(2) broadly allows a code of practice "to regulate" the collection, use and disclosure of, and procedures for dealing with, personal information held by an agency. On the other hand, s 30(1) allows a code of practice "to modify the application of" the IPPs.

7.13 This gives rise to an ambiguity, as it would seem that s 29(2) allows a privacy code of practice to do more than merely modify the application of the IPPs to an agency. It is arguable that a disclosure of personal information authorised by a code of practice may constitute a "lawful excuse" for the purposes of many secrecy provisions.[12]

ISSUE 48

Should the interaction of s 29(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) with s 30(1) of that Act be clarified?

ISSUE 49

Should the precise scope of a privacy code of practice be clarified?

THE MEANING OF "PERSON" IN s 37 AND 38 OF PPIPA

7.14 The meaning of the word "person" in Part 4 of PPIPA, particularly in s 37 and 38, may need clarification and its use in those sections made consistent. Sections 59 and 60 in Part 7 of HRIPA are equivalent sections. However, HRIPA differs from PPIPA in one small but significant way, which is described below.

7.15 Section 37 of PPIPA gives a general authority to the Privacy Commissioner "in connection with the exercise of [his or her] functions" to "require any person or public sector agency" to give or

12. The qualification in s 22 of the *Privacy and Personal Information Protection Act 1998* (NSW), which provides that nothing in the provisions relating to exemptions authorises an agency to do anything otherwise prohibited, does not apply to privacy codes of practice.

produce certain statements or documents.[13] Section 38(4) of PPIPA, on the other hand, relates to an inquiry or investigation being conducted by the Privacy Commissioner. It provides that, in those circumstances, the Privacy Commissioner must set aside any requirement to give or produce a statement or document "if it appears to the Privacy Commissioner that the person concerned does not consent ..." No mention is made of a "public sector agency". Sections 38(5) and (6) also only refer to a "person". By contrast, s 59 and 60 of HRIPA both refer to a "person or organisation".

7.16 The Crown Solicitor has noted that "[t]he purpose of PPIPA would suggest that 'person' in s 37 ought to have a wider meaning than a natural person, given the limited definition of 'public sector agency'[14] (and having regard to the definition of 'person' in s 21(1) of the *Interpretation Act 1987*)".[15] However, this is not necessarily what Parliament intended and it may be that the provisions are to be read narrowly so that the meaning of "person" is a "natural person".

7.17 More importantly, it is difficult to see why, as a matter of fair operation, s 38(4) should not require the Privacy Commissioner to set aside a requirement to give a statement, produce a document or answer a question if *an agency* does not consent to compliance and could not be compelled in court proceedings to give or produce the evidence. It cannot be assumed that the reference to "person" in s 38(4) includes a representative/employee of a public sector agency as s 37 makes specific and separate reference to "public sector agency". This interpretation is supported by the fact that HRIPA, drafted several years after PPIPA, makes s 60(4), the equivalent provision to s 38(4), apply specifically to a "person or organisation".

ISSUE 50

Should the word "person" in s 37 and 38 of the *Privacy and Personal Information Protection Act 1998* (NSW) be read as meaning a "natural person"? If so, should this be clarified in the legislation?

ISSUE 51

Should both s 37 and 38(4) of the *Privacy and Personal Information Protection Act 1998* (NSW) apply to a "person or public sector agency"?

---

13. This authority is qualified by s 37(2) of the *Privacy and Personal Information Protection Act 1998* (NSW).
14. See *Privacy and Personal Information Protection Act 1998* (NSW) s 3.
15. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.65]. "Person" includes an individual, a corporation and a body corporate or politic: *Interpretation Act 1987* (NSW) s 21(1).

PUBLIC INTEREST DIRECTIONS - PPIPA s 41 ; HRIPA s 62

7.18 Section 41 of PPIPA and s 62 of HRIPA, respectively, allow the Privacy Commissioner to make a written direction that an agency/organisation is not required to comply with an IPP or HPP or a privacy code of practice or health privacy code of practice, or that the application of an IPP, HPP or code to an agency is to be modified, providing he or she is satisfied that the public interest in so directing outweighs the public interest in compliance with the IPP, HPP or code.

7.19 The Crown Solicitor has pointed out that s 41 of PPIPA contains no mechanism for amendment of a direction.[16] Nor does s 62 of HRIPA. It would seem, therefore, that a direction, once issued, cannot be amended and a new direction must be issued, revoking the earlier one. The Privacy Commissioner could rely on s 48(1) of the *Interpretation Act 1987* (NSW) for the power to do this.[17] The question arises, however, whether it would not be simpler and clearer to include a sub-section in s 41 of PPIPA and in s 62 of HRIPA giving the Privacy Commissioner the power to amend an earlier direction.[18]

PROPOSAL 17

Section 41 of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 62 of the *Health Records and Information Privacy Act 2002* (NSW) should be amended to give the Privacy Commissioner the power to amend an earlier direction.

7.20 In addition, the Crown Solicitor has pointed out that, unlike privacy codes of practice, s 41 of PPIPA does not state that a direction can apply to a class of public sector agency.[19] Again, this comment is applicable to s 62 of HRIPA. There is a view that the section cannot be read as encompassing a class of agency and the Commission agrees with this. The public interest question is integral to the exercise of the discretion to make a direction and would become too diluted if exempting an entire class of agency from compliance with an IPP, HPP or code was under consideration. We do not believe that Parliament intended the power given by s 41 and s 62 to be so broad. Nevertheless, we invite community response as to the interpretation of s 41 of PPIPA and s 62 of HRIPA and whether the section should be

---

16. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.68].
17. Section 48(1) provides: "If an Act or instrument confers or imposes a function on any person or body, the function may be exercised (or, in the case of a duty, shall be performed) from time to time as occasion requires."
18. Compare s 31(7) of the *Privacy and Personal Information Protection Act 1998* (NSW).
19. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.70].

clarified, either to deny or allow application to a class of public sector agency/organisation.

ISSUE 52

(a) Should the intended application of s 41 of the Privacy and Personal Information Protection Act 1998 (NSW) and s 62 of the Health Records and Information Privacy Act 2002 (NSW) be clarified?

(b) Should the sections make clear that the Privacy Commissioner may make a written direction applying to a class of agency/organisation?

(c) Alternatively, should the sections make clear that the Privacy Commissioner may not make a written direction applying to a class of agency/organisation?

COMPLAINTS UNDER s 45 OF PPIPA

Complaints on behalf of the individual

7.21 Section 45(1) of PPIPA does not identify who may make a complaint ("a complaint may be made") and does not appear to limit its application to the individual concerned. However, a *Privacy NSW Complaints Protocol* was issued stating that the Privacy Commissioner had received legal advice to the effect that the section is limited to an individual whose privacy has been violated.[20] This would include a third party acting on behalf of the individual, but not a third party whose privacy has not been affected, such as a "whistleblower".

ISSUE 53

Should s 45(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to clarify that its application is limited to an individual whose privacy has been violated, or a person acting on behalf of the individual?

Criteria to be applied by the Privacy Commissioner

7.22 Section 45(1) of PPIPA provides that a "complaint may be made to (or by) the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual". The Act provides no guidance as to what matters the Privacy Commissioner may take into account in assessing and dealing with complaints under s 45(1),

20. *Privacy NSW Complaints Protocol* (issued 22 July 2002, revised July 2006), [2.2.2].

although these are set out in detail in the *Privacy NSW Complaints Protocol*.

7.23 The Crown Solicitor suggests that what might constitute "violation of" and "interference with" an individual's privacy could usefully be clarified.[21] One possibility is to model standards for assessing the alleged violation or interference on the Data Protection Principles. However, the counter argument is that the Data Protection Principles should not be used as a substitute for the application of the test in s 45(1),[22] as they, and the analogous IPPs, appear to represent different notions of privacy. It seems unlikely that Parliament would have intended that the obligations and prohibitions applied to public sector agencies by the IPPs could be indirectly applied to other persons through s 45(1).

ISSUE 54

Should the meaning of "violation of" and "interference with" an individual's privacy in s 45(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) be clarified?

ISSUE 55

Should the legislation provide guidelines as to what can be taken into account in determining whether there has been a "violation of, or interference with, the privacy of an individual"?

Relationship between s 45 and s 36(2)(k) of PPIPA

7.24 Section 36(2)(k) of PPIPA sets out one of the Privacy Commissioner's functions as being "to receive, investigate and conciliate complaints about privacy related matters". Section 45(1) of PPIPA provides that "a complaint may be made to (or by) the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual".

7.25 It is unclear how these sections fit together; in particular, whether or not they provide independent sources of power. If the sections should not be regarded as separate and independent sources of power, the question remains as to how to reconcile the broad and milder wording of s 36(2)(k), which only requires that a matter be privacy related, and the more specific language of s 45(1), which requires a "violation of" or "interference with" privacy. The Commission is interested to receive submissions on whether the

21. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.57].
22. The test being that the Privacy Commissioner may make or receive a complaint if there has been a "violation" or "interference".

differences between the sections have caused difficulties or uncertainties in their application, to determine whether clarification is called for.

ISSUE 56

(a) Does the interaction between, and operation of, s 45 and 36(2)(k) of the *Privacy and Personal Information Protection Act 1998* (NSW) need to be clarified?

(b) Should these sections be regarded as together regulating the Privacy Commissioner's functions and powers with respect to complaints or as two independent sources of the Privacy Commissioner's powers?

Application of s 51 of PPIPA to withdrawn complaints

7.26 Section 51 of PPIPA provides that, even though the Privacy Commissioner declines to deal with a complaint, or refers the complaint to a relevant authority, the Privacy Commissioner may still conduct an inquiry or investigation into any general issues raised by the complaint.

7.27 The Crown Solicitor has suggested that it is unclear whether, if a complaint is withdrawn under s 45(6) of PPIPA, the Privacy Commissioner can still conduct an inquiry or investigation into the complaint pursuant to s 51.[23] The Crown Solicitor points out that s 51 expressly deals with two of the scenarios that can follow the making of a complaint (the Privacy Commissioner declines to deal with the complaint - s 46(3); or refers it to a relevant authority – s 47), but not the other two possible scenarios (the complaint is withdrawn – s 45(6); it is dealt with under s 48(1)). Given the express wording of s 51, the Commission is of the view that it is not intended to apply to other scenarios, in particular, where a complaint is withdrawn. At this stage, we see no need for amendment of this section, but invite submissions on the point.

ISSUE 57

Does s 51 of the *Privacy and Personal Information Protection Act 1998* (NSW) require clarification with respect to the Privacy Commissioner's power to conduct an inquiry or investigation into any general issue raised by a withdrawn complaint?

23. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.61].

Report to Parliament under s 65 of PPIPA

7.28 Section 65 of PPIPA allows the Privacy Commissioner to make a "special report" to Parliament "on any matter arising in connection with the discharge of his or her functions". The Privacy Commissioner clearly has a basis for making a report under s 65 in relation to a complaint as his or her functions include "to receive, investigate and conciliate complaints about privacy related matters (including conduct to which Part 5 applies)".[24] Nevertheless, the Crown Solicitor has suggested that it is unclear whether s 65 extends to allowing a report relating to a complaint made under s 45.[25]

7.29 It could be argued that it does not, on the basis that s 50 already expressly deals with reports that the Privacy Commissioner may make in relation to a complaint. However, s 50 allows the Privacy Commissioner to make a report as to any findings or recommendations made by him or her but only in relation to a complaint dealt with by him or her. Section 46, on the other hand, envisages that not all complaints made to or by the Privacy Commissioner under s 45 will be dealt with by the Privacy Commissioner. In that case, without s 65, the Privacy Commissioner may be precluded from reporting to Parliament on a matter of concern to him or her arising out of the complaint. There can be no merit in, or justification for, this consequence.

7.30 In addition, the Commission is not convinced that a power to make a "special report" to Parliament is inconsistent with the discretion given to the Privacy Commissioner under s 50 to "make a written report as to any findings or recommendations … in relation to a complaint". Nor does s 50 appear to preclude the making of a special report to Parliament in addition to a report made under that section. More particularly, the primary purpose of s 50 is impliedly to inform the complainant of the outcome of the complaint and also to inform "such other persons or bodies as appear to be materially involved in matters concerning the complaint".[26] While Parliament may be interested in matters of general public interest and concern that arise out of the complaint, strictly speaking, Parliament could not be said to be "materially" interested.

---

24. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(k). Part 5 of the *Privacy and Personal Information Protection Act 1998* (NSW) deals with internal reviews of conduct by public sector agencies.
25. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.63].
26. *Privacy and Personal Information Protection Act 1998* (NSW) s 50(2).

ISSUE 58

(a) Is it correct to conclude that the Privacy Commissioner has the power to make a "special report" under s 65 of the *Privacy and Personal Information Protection Act 1998* (NSW) in relation to a complaint made under s 45, in addition to the power to make a report under s 50 of that Act?

(b) Should the legislation be amended to clarify the Privacy Commissioner's powers under s 65 and s 50 of the *Privacy and Personal Information Protection Act 1998* (NSW) to make a report relating to a complaint made under s 45?

REVIEW OF CONDUCT BY THE ADT - PPIPA PART 5; HRIPA s 21

Nature of the jurisdiction

7.31 Does the ADT hear PPIPA matters in its original or review jurisdiction? The ADT may make "original decisions" or "review reviewable decisions".[27] An "original decision" is "a decision of the Tribunal made in relation to a matter over which it has jurisdiction under an enactment to act as the primary decision-maker".[28] A "reviewable decision" is "a decision of an administrator that the Tribunal has jurisdiction under an enactment to review".[29]

7.32 The relevance of determining this question is that the ADT has different powers available to it depending on the jurisdiction. For example, in its "review" jurisdiction, but not in its "original" jurisdiction, the ADT has the power to award costs. There are also some differences in the rules that apply to each jurisdiction.

7.33 Although the ADT has held that applications to it under PPIPA fall within the ADT's review jurisdiction,[30] it has observed that the

27. *Administrative Decisions Tribunal Act 1997* (NSW) s 36(1).
28. *Administrative Decisions Tribunal Act 1997* (NSW) s 7.
29. *Administrative Decisions Tribunal Act 1997* (NSW) s 8.
30. *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132. The ADT found a number of indications that this is what Parliament intended: s 52(4) of the *Privacy and Personal Information Protection Act 1998* (NSW) ousts the application of s 53 (Internal reviews) of the *Administrative Decisions Tribunal Act 1997* (NSW); s 55(3) of the *Privacy and Personal Information Protection Act 1998* (NSW) provides that nothing in s 55 limits the ADT's powers under div 3, pt 3, ch 5 of the *Administrative Decisions Tribunal Act 1997* (NSW); the ADT only has power to award costs in its review jurisdiction.

legislative intention of PPIPA "is not consistent"[31] and has acknowledged that there is a lack of clarity on the issue.[32] The ADT has also observed that "the PPIPA jurisdiction does not fit comfortably into either category".[33]

7.34 By way of comparison, the Note to s 48(1) of HRIPA clearly states that the ADT exercises "original" jurisdiction when hearing applications for an inquiry into a complaint made to the Privacy Commissioner under that Act.

7.35 The Crown Solicitor has raised a possible argument that because s 55 of PPIPA confers a right to apply to the ADT for a review of the "conduct that was the subject of the application [for internal review] under section 53",[34] and not the agency's determination, there has been no "reviewable decision".[35]

7.36 On one view, it is difficult to see how s 63 of the *Administrative Decisions Tribunal Act 1997* (NSW) ("ADT Act") can be applied to a review of "conduct". Section 63 provides that in determining an application for review of a reviewable decision, the ADT is to decide what is "the correct and preferable decision". The counterargument is that, as the definition of "decision" in s 6(1)(g) of the ADT Act includes "doing or refusing to do any other act or thing", this is wide enough to include the types of conduct set out in s 52(1) of PPIPA. Further, "conduct", as described in Part 5 of PPIPA may be a "decision" or some act or omission. As well, a public sector agency can be said to be an "administrator" for the purpose of s 8 of the ADT Act.[36]

7.37 Whether the jurisdiction is classified as "original" or "review", the ADT is "strongly of the view" that cases before it "need to be approached in a way that is equivalent to how [it handles] 'merits review' work".[37] It does not accept the view that "the merits review

31. *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [12].
32. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (26 May 2004), 3.
33. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 10.
34. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(1).
35. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.76].
36. Section 9 of the *Administrative Decisions Tribunal Act 1997* (NSW) defines an "administrator" as "the person or body that makes (or is taken to have made) the decision under the enactment concerned".
37. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 11.

jurisdiction can only apply to reviewable decisions".[38] However, it is concerned that if the jurisdiction is classified as being "original", it would follow that "a civil litigation model should apply".[39] It points out that, in reality, cases brought before the ADT under PPIPA deal with the administrative conduct of an agency, which, in the ADT's view, is no different from putting in issue an administrative decision. In that case, the same protocols should apply, such as: that no burden of proof rests on one party over another; that the ADT's task is to determine what the "correct and preferable" approach might have been; and to do so having regard to the IPPs.[40]

ISSUE 59

(a) Should s 55 of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to clarify whether an application to the Administrative Decisions Tribunal is heard in its original or review jurisdiction?

(b) Should the jurisdiction be specified as being "review"?

Absence of a limitation period for review by the ADT

7.38 While an application for internal review by an agency must be made within six months from the time the applicant became aware of the conduct complained of,[41] there is no time limit on applying to the ADT for review of an internal review pursuant to s 55 of PPIPA.[42] Under HRIPA, a person who has made a complaint against a private sector person to the Privacy Commissioner can apply to the ADT for an inquiry into the complaint, providing this is done within 28 days

38. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 11.
39. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 11.
40. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 11.
41. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(3)(d).
42. *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [19]: "Even applying a purposive approach to statutory interpretation, it is not possible to read into s 55 of the [*Administrative Decisions Tribunal Act 1997* (NSW)], or any other provision, a time limit for applications to the Tribunal under the PPIP Act. There is only one possible construction of the provisions set out above, and that is that there are no time limits for the lodging of privacy applications with the Tribunal."

after: receiving the Privacy Commissioner's report; or a day nominated in the report as the day after which an application may be made.[43]

7.39 In the Crown Solicitor's view, the absence of a limitation period for review under PPIPA has the potential to prejudice an agency, particularly as the ADT does not enforce any rule that the applicant bears the onus of proof.[44] It considers that the rule that neither the applicant nor the respondent agency carries a burden of proof to prove or disprove a fact applies to its review proceedings.[45] Theoretically, an applicant could apply to the ADT years after an agency has carried out an internal review, and with the applicant bearing no onus of proving or disproving facts, the agency is faced with considerable difficulty producing witnesses and documentation to defend its conduct.

7.40 The ADT itself supports the introduction of a time limit on filing an application for review in the Tribunal.[46] It suggests that 60 days after completion of the internal review would be an appropriate time limit. Concurrently with such an amendment, the ADT submits that a provision should be added allowing a person who lodges a complaint with the Privacy Commissioner pursuant to s 45 of PPIPA within time to preserve a right to apply to the ADT for external review until after the s 45 process is completed.[47] The ADT also advocates allowing out-of-time requests for an internal review.[48]

43. *Health Records and Information Privacy Act 2002* (NSW) s 48.
44. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.81].
45. See *GR v Director-General, Department of Housing* [2004] NSWADTAP 26, [35] and [36]. Although, an application may be dismissed if the application produces insufficient evidence of circumstances that might warrant a finding of unlawful conduct where those circumstances are within the knowledge of the applicant but not known to the agency: *FY v Commissioner, Health care Complaints Commission* [2003] NSWADT 128.
46. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 9.
47. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 9. See s 54 of the *Freedom of Information Act 1989* (NSW).
48. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 9.

PROPOSAL 18

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a limitation period for application for review by the Administrative Decisions Tribunal of an internal review. This should provide that an application to the Administrative Decisions Tribunal for external review of a complaint must be made within 60 days after the applicant:

(a) is notified that the Privacy Commissioner refuses to investigate the conduct complained of; or

(b) receives a report of the results of the Privacy Commissioner's investigation.

ISSUE 60

Should s 53(3) of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to include a provision allowing a person to request internal review of conduct outside the six-month limitation period?

The ADT's powers on review

7.41 Where an application has been made for internal review of an agency's conduct, s 55(2) of PPIPA provides that the ADT may decide not to take any action on the matter or may make any of the orders listed "on reviewing the conduct". The section does not require that the ADT make a finding that the conduct has breached the provisions of PPIPA before granting one of the listed remedies.

7.42 The Crown Solicitor has argued that it cannot be implied that a reference to "conduct" in s 55(2) is a reference to conduct in breach of an IPP or a privacy code of practice, or that it is a disclosure of private information kept in a public register, (s 51(1) conduct)[49] because s 52(2) defines "conduct" to include "alleged conduct".[50]

7.43 The Crown Solicitor has concluded that it is likely that s 55(2) would be construed purposively so that an order could only be made in respect of infringing conduct and not merely alleged conduct, but that this should be clarified.[51] The Commission agrees that the effect of the section should be to give the ADT power to make orders only on finding that conduct of a type specified in s 52(1) of PPIPA has occurred, and not merely following his or her review of alleged conduct. We agree that the section should be amended to clarify this.

---

49. Section 52(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) specifies that this is the conduct to which Part 5 applies.
50. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.82].
51. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [3.82].

PROPOSAL 19

Section 55(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that the Administrative Decisions Tribunal may make any one or more of the orders listed in subsections (a)-(g) on finding that the public sector agency's conduct the subject of the review was conduct that:

- contravened an IPP that applied to the agency;
- contravened a privacy code of practice that applied to the agency; or
- amounted to disclosure by the agency of private information kept in a public register.

7.44 We note that s 53(7) of PPIPA is similarly worded so as to permit an agency that undertakes internal review of its conduct to take remedial action "following the completion of the review", without reference to the making of any findings. However, there are not the same implications as with s 55(2) as it is the agency's own decision to make amends for its own conduct, whether or not it accepts that the conduct has caused harm. This is in contrast to the possibility of a tribunal making orders against an agency, despite there being no finding of misconduct.

Role of the Privacy Commissioner

7.45 The ADT has drawn attention to an argument that the Privacy Commissioner does not have a right to appear before the Appeal Panel of the ADT. Although the Appeal Panel has rejected this argument, the ADT submits that it would perhaps be desirable to amend PPIPA to clarify this point.[52] The Commission agrees that, as s 55(7) of PPIPA makes it clear that the Privacy Commissioner has a right to appear in proceedings before the ADT, there should be legislative consistency in s 56.

52. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 9.

PROPOSAL 20

Section 56 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a provision that the Privacy Commissioner has a right to appear and be heard in any proceedings before the Appeal Panel of the Administrative Decisions Tribunal.

Commissioner Determination model vs Tribunal Determination model

7.46 Looking at the resolution of complaints from a broad perspective, the ADT questions whether a final determination by the Tribunal is the best model.[53] Although the ADT prefers final determination by the Privacy Commissioner, it acknowledges that there is divided opinion on this question. The Commissioner Determination model has been adopted in privacy legislation in the Canadian federal jurisdiction and in a number of Canadian provinces and in Freedom of Information legislation in Queensland and Western Australia. The Tribunal Determination model has been adopted in privacy legislation in the Commonwealth *Privacy Act*, in New South Wales, Victoria, the United Kingdom and New Zealand.

7.47 The ADT considers that the specialisation of the office of Privacy Commissioner, and the access to more flexible resources that goes with the office, is the main advantage of the Commissioner Determination model.[54] The current President of the ADT was formerly the Federal Privacy Commissioner and is in a unique position to compare his direct experience with each model of final determination of complaints. He relates that, as Federal Privacy Commissioner, he had an experienced investigative staff that had credibility with the agencies "and knew how to deal neutrally and impartially with complainants and agencies".[55] He observes that "this was an agency-driven approach to the task that is left in Tribunals largely to the parties".[56]

53. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 7.
54. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 7.
55. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 7.
56. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 7.

7.48 By contrast, the ADT has no investigative staff and "does not undertake full, professional investigation of complaints". (It could not have an activist investigative arm if public confidence in the ADT to be independent and detached is to be maintained, even if limited to privacy cases.)[57]

7.49 The NSW Department of Health has expressed concerns with the current Tribunal Determination model, arguing that the process, compared with complaints that are mediated, is complicated and expensive.[58] It believes that the incidence of self-represented litigants in the ADT protracts proceedings. In its experience, many of the cases that end up in the ADT are the minor ones where the Department of Health is disputing a technical point, whereas relatively major cases are more often mediated.

7.50 Changing PPIPA's Part 5 review of conduct process to give final determination of a complaint to the Privacy Commissioner rather than the ADT would be a significant departure. However, this is the opportunity to make major reforms and accordingly the Commission puts forward the issue for debate.

ISSUE 61

Should Part 5 of the *Privacy and Personal Information Protection Act 1998* (NSW) be amended to give final determination of a complaint to the Privacy Commissioner rather than the Administrative Decisions Tribunal?

57. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998,* 7.
58. Department of Health, *Consultation* (3 December 2007).

8. Relationship between PPIPA and other legislation

- Introduction
- The relationship between PPIPA and the *FOI Act*
- The relationship between PPIPA and the SRA

INTRODUCTION

8.1 This chapter is concerned with the relationship between the *Privacy and Personal Information Protection Act 1998* (NSW) ("PPIPA") and other statutes that contain provisions dealing with privacy and access to information. The fact that privacy in New South Wales is currently regulated by several Acts has given rise to confusion about the way in which these pieces of legislation interact with one another.

8.2 Specifically, the chapter deals with the following:

- the relationship between PPIPA and the Freedom of Information Act 1989 (NSW) ("FOI Act"), including:
- duplication and inconsistencies between the information disclosure, access and collection provisions;
- inconsistencies between the complaints-handling and review provisions found in the two Acts; and
- arguments for and against amalgamation of the oversight of privacy and FOI;
- the relationship between PPIPA and the Local Government Act 1993 (NSW) ("LGA");
- the relationship between PPIPA and the State Records Act 1998 (NSW) ("SRA").

8.3 The Acts listed above do not exactly replicate one another in privacy regulation, as each has its own particular focus and priorities, reflected in the different objects and purposes of each Act. The LGA is concerned with the structure and functions of councils, while the SRA has the very different role of governing the management of public offices' records. Unlike PPIPA, neither is primarily designed to regulate privacy and access to information. However, particular provisions in the various pieces of legislation relating to access to information held by government agencies cover essentially the same ground, meaning that more than one regulatory regime may apply in particular circumstances.

8.4 In fact, there are three separate regimes governing access to, and amendment of, documents held by public sector agencies: the LGA for councils; and PPIPA and the FOI Act for both councils and other

public sector agencies in New South Wales.[1] In addition, the SRA contains provisions that bear on the issue.

8.5 The relevant provisions in these Acts often regulate the same thing but they do so in terms that are, at best, only similar or comparable to each other, not identical. At worst, it has been suggested that the differences between the Acts are such that it "is simply not possible" to obey them at the same time.[2] The former Privacy Commissioner has said that the provisions in PPIPA, the FOI Act and the SRA "are in fact, in a number of key respects, insufficiently compatible, [so] that an officer will have to be in breach of one of them at some stage".[3]

8.6 In a similar vein, the Ombudsman has noted that the three regimes are "largely incompatible"[4] and have led to "considerable confusion for both users and the public officials responsible for administering the relevant legislation".[5] These concerns were echoed by other submissions to the Attorney General's Review of PPIPA,[6] including those made by Sydney University, Bankstown Council, the Department of Education and Training, the Ministry for Police and the Roads and Traffic Authority.

8.7 The major overlap is between PPIPA and the FOI Act.

THE RELATIONSHIP BETWEEN PPIPA AND THE FOI ACT

Disclosure, access and correction provisions

8.8 This section analyses the duplication of, and inconsistencies between, the provisions of PPIPA and the provisions of the FOI Act that deal with disclosure and correction of, and access to, information. These are s 13-15 of PPIPA and Parts 2-4 of the FOI Act.

1. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (April 2004), 14.
2. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 16, quoting former Privacy Commissioner Chris Puplick.
3. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 16, quoting former Privacy Commissioner Chris Puplick.
4. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 15.
5. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 14.
6. New South Wales AttorneyGeneral's Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly).

8.9 It is because the relevant provisions of the two Acts are similar, not identical, that the duplications produce inconsistencies. In particular, differences in terminology result in substantive differences in application. For example, while the FOI Act is limited in its application to “documents”,[7] PPIPA applies to “information”,[8] which is a wider term than “documents” because information includes what has not been recorded in documentary form.[9] On the other hand, PPIPA applies only to “personal information”,[10] whereas the FOI Act allows access to a wide range of documents held by an agency.

8.10 Applicants and agencies will enjoy different benefits, and incur different obligations, depending on the particular statute under which the application for access to information is dealt with. This might not matter if the two statutes simply operated concurrently, or in parallel, without affecting each other. But they do not. Particular provisions in the Acts complicate their interaction. While PPIPA is not intended to affect the FOI Act, the FOI Act specifically affects PPIPA through the operation of s 20(5) of PPIPA. However, the way in which it does so is not entirely clear because, as discussed in Chapter 6 in paragraph 6.32, the correct interpretation of that section is uncertain.

8.11 Section 20(5) of PPIPA provides that “the provisions of the [FOI Act] 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”.

8.12 Privacy NSW has argued that it is uncertain exactly how “the access and correction provisions of the FOI Act relate to or are imported into” PPIPA.[11] The Ombudsman agrees that the provision is “ambiguous” but that it seems to mean that if disclosure, access or correction rights may be validly denied under the FOI Act (under Parts 2–4) they may be similarly denied under PPIPA (s 13–15).[12] Thus, an application for access to information under s 14 of PPIPA

---

7. *Freedom of Information Act 1989* (NSW) s 16.
8. *Privacy and Personal Information Protection Act 1998* (NSW) s 4.
9. Section 4 of the *Privacy and Personal Information Protection Act 1998* (NSW) provides that “personal information means information or an opinion (including information or an opinion forming part of a database and whether or not recoded in material form) …”.
10. Defined as “information or an opinion … about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion”: *Privacy and Personal Information Protection Act 1998* (NSW) s 4(1).
11. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998* (June 2004), 82.
12. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 19.

may be refused because of conditions and limitations (on s 16 of the FOI Act) found in Part 3 of the FOI Act. The Crown Solicitor, on the other hand, remarked that "[t]he difficulty [of interpretation] lies in identifying the provisions of the FOI Act that impose 'conditions or limitations (however expressed)' with respect to any 'matter' referred to in ss 13, 14 or 15", noting that it was highly unlikely that *all* the provisions affecting the access right under the FOI Act would have been intended to apply to those seeking access to information under s 14 of PPIPA.[13]

8.13 It is not difficult to see why the FOI Act and PPIPA have created such confusion. There is a fundamentally different policy underlying each Act:

> Privacy and data protection laws are intended to protect and promote the fair handling of personal information by agencies, whilst FOI laws are intended to promote open government in relation to handling of personal and non-personal information.[14]

8.14 The President of the Administrative Decisions Tribunal and former Federal Privacy Commissioner, Judge Kevin O'Connor, has commented that where jurisdictions have FOI and privacy laws, frequently both provide for access to, and amendment of, personal information, as a result of which there are often "tensions between the two laws because of differences in language and approach".[15] In his view, there is a "good case" for there being "one provision in New South Wales law that deals with the right of access, and one provision that deals with the right of amendment". He has observed that, in contrast, what we have now is "a situation where differently expressed rights are found in FOI and Privacy statutes bearing on the one set of records". His conclusion is that: "[t]his should be rationalised". [16]

8.15 The Ombudsman has queried whether all the IPPs need to be implemented solely under PPIPA, or whether it might not be better for the three relevant IPPs (in s 13, 14 and 15) to be implemented through the provisions of the FOI Act "(with or without any appropriate amendment to that Act)".[17] This would avoid the duplications and

---

13. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), 24.
14. *Ormonde v NSW National Parks & Wildlife Service (No 2)* [2004] NSWADT 253, [56].
15. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (26 May 2004), 8.
16. New South Wales, Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998*, 9.
17. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 14.

inconsistencies between the two Acts and the over-complexity of the regulatory regime.

8.16 The Ombudsman has proposed the following solution "to address the proliferation of access to information regimes and to help simplify the current complex regulatory environment":[18]

> 1) repeal s 20(5) of [PPIPA]
>
> 2) as originally proposed in the [PPIP] Bill that went to Parliament, amend s 13–15 and/or s 20 of [PPIPA] to provide that the [IPPs] set out in s 13–15 do not apply to agencies to which the FOI Act appl[ies] and that in relation to those agencies those principles are implemented through the relevant provisions of the FOI Act, and
>
> 3) if considered necessary, amend the FOI Act to put beyond doubt that agencies can adopt informal methods of releas[ing] personal information to the person concerned.[19]

8.17 It may, at first glance, seem incongruous to pass legislation (namely PPIPA) to protect people's privacy of, and access to, personal information only to then pass an amendment to the Act that would seriously limit the scope of its application. Since the FOI Act is of general application, specifying that the rights of access granted by PPIPA do not apply to agencies governed by the FOI Act would severely restrict the extent of PPIPA's reach. However, this approach can be supported on the basis that if rights of access to information are sufficiently protected by the FOI Act, the superadded protection of PPIPA is unnecessary.

ISSUE 62

Should the disclosure, access and correction provisions of *the Privacy and Personal Information Protection Act 1998* (NSW) and the *Freedom of Information Act 1989* (NSW) be rationalised?

ISSUE 63

Should the Freedom of Information Act 1989 (NSW) be the means by which the *Privacy and Personal Information Protection Act 1998* (NSW) access rights are obtained?

---

18. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998*, 20.
19. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998*, 20–21.

Complaints-handling and review provisions

8.18 Both PPIPA and the FOI Act contain provisions governing how complaints about breaches of privacy (or issues related to access to information) are to be handled, and what mechanisms are available for review by an agency of any decision made relating to any such complaint. There are significant differences between the two Acts. Some of the key differences are as follows:

- A person who makes a complaint to the Privacy Commissioner under PPIPA and is dissatisfied with the result cannot take the matter to the Administrative Decisions Tribunal ("ADT") whereas a person who complains to the Ombudsman under the FOI Act can.
- Areas of complaint under PPIPA are confined to: alleged violations of, or interferences with, the privacy of an individual;[20] an agency's contravention of an IPP or a privacy code of practice; and the disclosure of personal information kept in a public register.[21] On the other hand, complaints under the FOI Act can be made about conduct of any person or body in relation to a determination made by an agency under the FOI Act.[22]
- A complaint to the Privacy Commissioner can be made concurrently with a review application to the ADT, but the Ombudsman will not investigate a complaint under the FOI Act while proceedings are before the ADT.[23]
- The Privacy Commissioner has a right to appear and be heard in any proceedings before the ADT in relation to a review under s 55 of PPIPA, but the Ombudsman has no such right under the FOI Act.
- Under PPIPA, neither the applicant nor the respondent agency carries a burden of proof to prove or disprove a fact before the ADT, but under the FOI Act, the onus of proof is on the respondent.[24]

8.19 When an aggrieved person applies to have an agency review its conduct under s 53 of PPIPA, the agency must notify the Privacy Commissioner of the application, keep him or her informed of the progress of the internal review and inform him or her of any findings

20. *Privacy and Personal Information Protection Act 1998* (NSW) s 45(1).
21. *Privacy and Personal Information Protection Act 1998* (NSW) s 52(1).
22. *Freedom of Information Act 1989* (NSW) s 52(1).
23. *Freedom of Information Act 1989* (NSW) s 52 and 53.
24. *Freedom of Information Act 1989* (NSW) s 61.

or determinations made in relation to the matter.[25] No similar provisions are made for the Ombudsman in the FOI Act.

8.20 Time limits for complaints and applications for internal review are also different under the two statutes:

- Under PPIPA, the applicant for internal review has six months from the time the applicant first became aware of the conduct complained of.[26] Under the FOI Act, the applicant has only twenty-eight days from the time notice of the determination is given to apply for an internal review.[27]
- Under PPIPA, a complainant has six months (from becoming aware of the relevant conduct) within which to make a complaint to the Privacy Commissioner.[28] Under the FOI Act, no time limit for complaining to the Ombudsman is imposed.
- Under PPIPA, applications for review by the ADT need not be made within any specified time limit. Under the FOI Act, applications must be made within sixty days of the agency's determination or the Ombudsman's decision.[29]

ISSUE 64

Should the complaints-handling and review procedures of *the Privacy and Personal Information Protection Act 1998* (NSW) and the *Freedom of Information Act 1989* (NSW) that are not specifically related to the particular provisions of each Act be made consistent?

Amalgamation of the oversight of privacy and FOI

8.21 One way of reducing the problem of duplications and inconsistencies between PPIPA and the FOI Act would be to charge a single body with the responsibility of overseeing the administration of both statutes. Privacy NSW's submission to the Attorney General's Review of PPIPA observed that this "makes intuitive sense": "[t]hey are two sides of the one coin in ensuring government agencies handle information in an accountable manner".[30] Its reasons for this view were threefold: the vast majority of FOI requests are for access to the applicant's own personal information; "one Information Commissioner is the trend in many common law jurisdictions"; and it would seem

---

25. *Privacy and Personal Information Protection Act 1998* (NSW) s 54(1).
26. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(3).
27. *Freedom of Information Act 1989* (NSW) s 34(2).
28. *Privacy and Personal Information Protection Act 1998* (NSW) s 45(5).
29. *Freedom of Information Act 1989* (NSW) s 54.
30. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 36.

desirable for a single individual to resolve tensions between FOI and privacy.[31]

8.22 The Ombudsman also supported amalgamating FOI and privacy functions. It commented that this would:

> provide a more integrated and coherent approach to information handling, fostering a better balance between the right to privacy with the need for a safe and open government. It would also reduce duplication, complexity and confusion for the public and agencies.[32]

8.23 Despite agreeing in principle, Privacy NSW and the Ombudsman disagreed on how an amalgamation of FOI and privacy should be implemented. Privacy NSW maintained that an amalgamation of functions should be under the auspices of an independent Information Commissioner. The Ombudsman, on the other hand, argued that it would make most sense for the role and responsibilities of the Privacy Commissioner to be absorbed into the Office of the Ombudsman.[33] It backed up its position with the following arguments:

- More people are aware of the existence and functions of the Ombudsman than are aware of the role of Privacy Commissioners, and people are therefore more likely to make a privacy complaint to the Ombudsman than to Privacy NSW.34
- The Ombudsman already has expertise in the area of privacy arising out of its roles in relation to police, community services, telecommunications interception, and so forth. Further, as it is a complaints-handling agency that already has jurisdiction in the related area of FOI, "integration of [Privacy NSW] into the Ombudsman would provide an opportunity to properly coordinate and integrate FOI and privacy practice, procedures and regulation."[35]

---

31. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 36.
32. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 27.
33. It submitted that "Privacy NSW should be amalgamated with the NSW Ombudsman, including: a) the transfer to the Ombudsman of the full staff and budget of Privacy NSW, and b) the establishment of a specialist access to information and privacy team within the NSW Ombudsman's Office": NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 28.
34. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 27.
35. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 27.

- Privacy NSW is too small to be viable as a stand-alone agency.[36]
- Most public sector agencies have delegated privacy and FOI responsibilities to the same staff.[37]

8.24 Privacy NSW put forward the following counter-arguments for not absorbing the office of the Privacy Commissioner into that of the Ombudsman:

- An Ombudsman should not be involved in policy-making and should be free to criticise bad policy.[38]
- The Australian Law Reform Commission recommended that the three roles of overseeing FOI, Privacy Commissioner and Ombudsman should remain separate, although it argued for cooperation between them.[39]
- Separate organisations might result in better accountability, as each could provide checks and balances on the other.[40]
- Jurisdictions that have appointed Information Commissioners have retained "a separate Ombudsman to deal with more general misconduct and maladministration in government".[41]
- Jurisdictions that have given the Ombudsman the role of regulating FOI have primarily limited the role to complaints-handling rather than wide policy-setting, advice or education roles. The role of Privacy Commissioner, on the other hand, is not so limited.[42]

8.25 The Ombudsman disputed a number of these assertions, especially those that contend that its primary role is complaints-

---

36. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 26.
37. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 27.
38. Privacy NSW noted that the Australian Law Reform Commission rejected the idea of an Ombudsman taking the role of FOI Commissioner for this reason: Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 36.
39. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 37.
40. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 37.
41. Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 37.
42. For example, Privacy NSW has a large, and growing, advice role and sees itself as a resource to agencies, not just a "watchdog": Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 37.

handling rather than oversight; and that the Ombudsman does not, or should not, have a role in policy development.[43]

8.26 The Ombudsman was also of the opinion that, even if Privacy NSW was not absorbed into its organisational structure, FOI and privacy still ought to be overseen by a single, separate agency, although it conceded that this would have "several serious shortcomings".[44] First, it submitted that "such a separate agency is unlikely to be viable on its own as it would only have a full time permanent staff of approximately 12 persons".[45] Secondly, there would still be overlap between the agency's role and that of the Ombudsman, especially in relation to FOI maladministration. The Ombudsman concluded that:

> there would therefore need to be adequate provision to enable that agency and the Ombudsman to share information, refer complaints or the issues arising out of complaints, coordinate concurrent investigations into related issues, etc.[46]

8.27 The Attorney General's Review of PPIPA raised an alternative view, noting that:

> [t]here 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).[47]

8.28 The Commission agrees with this view and is inclined, at this stage, not to recommend that the administration of FOI and privacy legislation be amalgamated in one body, but is interested in receiving submissions on the point.

ISSUE 65

Should the administration of Freedom of Information and privacy legislation be amalgamated in one body?

---

43. *Letter from the NSW Ombudsman to the Director, Legislation and Policy Division, NSW Attorney General's Department* (5 July 2004).
44. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 28.
45. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 28.
46. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 28.
47. New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, [13.12], 65.

THE RELATIONSHIP BETWEEN PPIPA AND THE LGA

8.29 A comparison of the FOI provision found in the LGA with similar provisions in the other statutes demonstrates that, while divergent terminology in different statutes can be the cause of inconsistencies and confusion (as it is in the case of PPIPA and the FOI Act), it is not always so in every respect. Consider the following provisions:

- Section 12(6) of the LGA provides that a council must allow inspection of its documents free of charge unless this would be contrary to public interest.[48]
- Section 14 of PPIPA provides that an agency that holds personal information must, at the request of the individual to whom the information relates, provide him or her with access to the information, without excessive delay or expense.[49]
- Section 16(1) of the FOI Act gives a person a right to access an agency's documents.[50]

8.30 Note that PPIPA and the FOI Act refer to a right of "access" to information or documents, whereas the LGA refers merely to a right of "inspection". On the face of it, this would appear to be something different (and less). However, a subsequent provision of the LGA that defines the right of inspection as including "the right to take away a copy of the document"[51] makes the right as extensive as the "access" rights granted in the other statutes. A difference in form (that is, the wording of the statute) is therefore not always determinative of a difference in substance (that is, the actual right conferred by the provision).

8.31 Nevertheless, the differences between the provisions of the LGA and those of PPIPA and the FOI Act are sufficiently significant and substantial to question the necessity for this legislative overlap. Since the application of both PPIPA and the FOI Act extends to councils, the problems of duplication and inconsistencies are simply reproduced and multiplied in the context of local government authorities, which are (as already observed) regulated by these two statutes in addition to the LGA.

8.32 An applicant for access to documents held by a council will therefore have a choice of proceeding under any or all of the three pieces of legislation, each with its own advantages and disadvantages. The Ombudsman has remarked that if the information sought is "simple, non-complex or non-contentious" it is better for both the

---

48. *Local Government Act 1993* (NSW) s 12(6).
49. *Privacy and Personal Information Protection Act 1998* (NSW) s 14.
50. *Freedom of Information Act 1989* (NSW) s 16(1).
51. *Local Government Act 1993* (NSW) s 12B(1).

applicant and the agency to deal with the application under PPIPA "because it has hardly any procedural requirements".[52] If, however, the information is more complex, extensive or contentious, applicants are likely to favour applying for access under the LGA, since "the options and discretions available to councils under that Act to refuse access to information are far more limited than under the FOI Act".[53] Councils themselves are likely to prefer to deal with applications for access to documents under the FOI Act because applicants have to submit their request in writing, councils can charge fees for the documents and "there are greater legal protections available for the council under the FOI Act than under either the [LGA] or PPIPA".[54]

8.33 The divergences and inconsistencies between PPIPA and the FOI Act were discussed above. The compounding of these by the addition of the LGA is illustrated in the following examples:

- The access right in PPIPA is limited to "personal information", while those in the LGA and FOI Act are not.
- Access to documents under the LGA is subject to a "public interest" test, but access under PPIPA or the FOI Act has no such test.
- Applications for information under the FOI Act must be in writing[55] and specify that they are being made under that Act[56] but there is no similar requirement under the LGA and PPIPA.
- if an agency refuses access to documents under the FOI Act, reasons for the refusal must be given to the applicant.[57] If an agency refuses access to an applicant under the LGA, reasons need not be given to the applicant but reasons must be given to the council.[58] If an agency refuses access to an applicant under PPIPA, reasons for the refusal need not be given at all (unless the decision is appealed to the ADT).

8.34 These are just some of the differences, inconsistencies and duplications between the three statutes.[59]

---

52. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 15.
53. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 20.
54. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 16.
55. *Freedom of Information Act 1989* (NSW) s 17(a).
56. *Freedom of Information Act 1989* (NSW) s 17(b).
57. *Freedom of Information Act 1989* (NSW) s 28(2)(e).
58. *Local Government Act 1993* (NSW) s 12A(1).
59. See NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* Appendix B-1, *Navigating the*

8.35 The NSW Ombudsman's submission to the Attorney-General's Review of PPIPA as to how the "proliferation of access to information regimes" should be addressed was quoted in paragraph 8.16 above. In substance, the submission argued for amendments that would ensure that the "access to information" provisions in PPIPA (s 13-15) did not apply to agencies to which the FOI Act's "access to information" provisions applied. Since the FOI Act applies to councils by defining an "agency" as including a council within the LGA, this exemption from the application of PPIPA would also extend to councils. They would, however, still be subject to two regulatory regimes (pursuant to the FOI Act and the LGA).

8.36 Whether this would satisfactorily resolve the current state of affairs needs to be examined. First, applicants would still have to choose from two separate statutes under which to make an access application to a local government authority. This would carry with it all the problems that the overlapping and competing regulatory regimes had before, albeit on a lesser scale. Secondly, it is debatable whether or not councils would prefer their legal obligations and responsibilities to be governed by the FOI Act rather than the LGA. The Local Government Governance Network Group, for example, submitted to the Attorney General's Review of PPIPA that the LGA should be the primary statute for managing council information, and if that submission were to be acted upon then the scope of the FOI Act would need to be reduced so as to exclude (or at least restrict or limit) its application to local authorities.

8.37 On the other hand, if, as the Ombudsman contends, there are greater protections when dealing with applications for access to information for councils and their staff under the FOI Act than under the LGA, then it would be understandable for councils to be arguing for the FOI Act to operate to the exclusion of the LGA. Either way, the eradication of all forms of duplication and overlap requires that any given agency (in this case, a council) be regulated by only one set of statutory provisions when dealing with applications for access to information.

Maze: A Guide to the Alternative Regimes for Access to Personal Information in NSW.

ISSUE 66

(a) Should the following amendments, as suggested by the NSW Ombudsman, be made?

- **repeal s 20(5) of the *Privacy and Personal Information Protection Act 1998* (NSW);**
- **amend s 13, 14 and 15 and/or s 20 of *the Privacy and Personal Information Protection Act 1998* (NSW) to provide that the IPPs contained in those sections do not apply to agencies to which the *Freedom of Information Act 1989* (NSW) applies and that, in relation to those agencies, those principles are implemented through the relevant provisions of the *Freedom of Information Act 1989* (NSW);**
- **amend the *Freedom of Information Act 1989* (NSW) to clarify that agencies can adopt informal methods of releasing personal information to the applicant.**

(b) Is there a better alternative to this solution?

ISSUE 67

What alternative amendments to *the Privacy and Personal Information Protection Act 1998* (NSW), the *Freedom of Information Act 1989* (NSW) and the *Local Government Act 1993* (NSW) would address the current problems arising from the application of three different regulatory schemes?

THE RELATIONSHIP BETWEEN PPIPA AND THE SRA

8.38 The main purpose of the SRA is "to make provision for the creation, management and protection of the records of public offices of the State and to provide for public access to those records".[60] Section 12 of the Act provides that "each public office must make and keep full and accurate records of [its] activities" and must "establish and maintain a records management program".[61] A "record" is defined to mean any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means".[62] A "state record" is defined to mean "any record made and kept, or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public office, or for the use of a public office,

60. *State Records Act 1998* (NSW), Long Title.
61. *State Records Act 1998* (NSW) s 12.
62. *State Records Act 1998* (NSW) s 3.

whether before or after the commencement of this section".[63] "Public office" is very widely defined and includes a State owned corporation.[64] Under the SRA, a person can gain access to State records that are at least 30 years old,[65] providing an open access direction has been made.[66]

8.39 The Crown Solicitor has highlighted an issue arising from the interaction between PPIPA and the SRA and their application to imperatives to amend or destroy documents.[67] Section 21(1) of the SRA prohibits a person from, among other things, disposing of, or altering, a State record. It is a prohibition that prevails over a provision of any other Act that was enacted before it commenced,[68] unless the conflicting Act provides expressly for its provision to have effect despite s 21 of the SRA.[69] The SRA (except for Part 4) commenced on 1 January 1999, whereas PPIPA was enacted on 30 November 1998.[70] However, disposal or alteration of a State record is not a contravention of s 21 if it is "done in accordance with normal administrative practice in a public office" or "authorised or required to be done by or under [the SRA], or by or under a provision of any other Act that is prescribed by the regulations as being an exception to [Part 3 of the SRA]".[71]

8.40 Section 12 of PPIPA provides that a public sector agency must not keep information for longer than is necessary and contemplates alteration of a document to delete information no longer needed or disposal of documents. The Crown Solicitor has submitted that it is unclear how s 12 was intended to apply in light of s 21 of the SRA. It notes that, to date, the ADT has declined to clarify the interaction between the provisions.[72] However, in *GR v Director-General, Department of Housing*, the ADT Appeal Panel stated that "every

63. *State Records Act 1998* (NSW) s 3.
64. *State Records Act 1998* (NSW) s 3.
65. *State Records Act 1998* (NSW) pt 6.
66. *State Records Act 1998* (NSW) s 51.
67. Crown Solicitor 's Office, New South Wales, *Advice* (5 October 2007), [6.1]-[6.4].
68. *State Records Act 1998* (NSW) s 21(6).
69. *State Records Act 1998* (NSW) s 21(7).
70. Although Part 2, Division 1 of the *Privacy and Personal Information Protection Act 1998* (NSW), containing the IPPs, did not commence until 1 July 2000.
71. *State Records Act 1998* (NSW) s 21(2).
72. See *FH v Commissioner, New South Wales Department of Corrective Services* [2003] NSWADT 72; and *GR v Director-General, Department of Housing* [2004] NSW ADTAP 26.

attempt should be made to read the provisions [of PPIPA and the SRA] harmoniously".[73]

8.41 Section 15(4) of PPIPA, on the other hand, specifically states that s 15 applies to public sector agencies despite s 21 of the SRA.

ISSUE 68

(a) Should a provision be inserted into s 12 of *the Privacy and Personal Information Protection Act 1998* (NSW), identical to that inserted into s 15(4) of that Act, providing that s 12, and any provision of a privacy code of practice that relates to the requirements set out in that section, apply to public sector agencies despite s 21 of the SRA?

(b) Alternatively, should s 12 be clarified as taking effect subject to the prohibition in s 21 of the *State Records Act 1998* (NSW)?

---

73. *GR v Director-General, Department of Housing* [2004] NSW ADTAP 26, [57].

Tables

- Table of cases
- Table of legislation

TABLE OF CASES

AW v Vice Chancellor, University of Newcastle [2008] NSWAD 86 .... 4.47, 6.51

Coco v The Queen (1994) 179 CLR 427 .... 5.6

Commissioner of Police, New South Wales v EG; *EG v Commissioner of Police, New South Wales* (GD) [2004] NSWADTAP 10 .... 5.14

Department of Education and Training v PN (GD) [2006] NSWADTAP 66 .... 5.42

Director General, Department of Education and Training v MT [2005] NSWADTAP 77 .... 6.44, 7.8

Edelsten v Investigating Committee of New South Wales (1986) 7 NSWLR 222 .... 5.99

EG v Commissioner of Police, New South Wales Police Service [2003] NSWADT 150 .... 5.43

FH v Commissioner, New South Wales Department of Corrective Services [2003] NSWADT 72 .... 8.40

Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW [2003] NSWADT 132 .... 7.33, 7.38

FY v Commissioner, Health Care Complaints Commission [2003] NSWADT 128 .... 7.39

GA v Department of Education and Training and New South Wales Police (GD) [2004] NSWADTAP 18 .... 5.6

GL v Director-General, Department of Education and Training [2003] NSWADT 166 .... 5.43

GR v Department of Housing [2003] NSWADT 268 .... 6.36

GR v Director-General, Department of Housing [2004] NSW ADTAP 26 .... 7.39, 8.40

HW v Commissioner of Police, New South Wales Police Service [2003] NSWADT 214 .... 5.65, 7.8

HW v The Director of Public Prosecutions (No 2) [2004] NSWADT 73 .... 6.21

JD v Department of Health [2005] NSWADTAP 44 .... 6.43

KD v Registrar, New South Wales Medical Board [2004] NSWADT 5 .... 5.58-5.59, 5.61

KO v Commissioner of Police (GD) [2004] NSWADTAP 21 .... 5.31

McKinnon v Secretary, Department of Treasury [2006] HCA 45 .... 2.28

McNamara v Consumer Trader and Tenancy Tribunal (2005) 221 CLR 646 .... 5.51-5.52

Miller v Miller (1978) 141 CLR 269 .... 5.99

NSW v Commonwealth [2006] HCA 52 .... 3.93

NW v Fire Brigades [2005] NSWADT 73 .... 5.16

NZ v Director General, New South Wales Department of Housing [2005] NSWADT 58 .... 6.43

OA v New South Wales Department of Housing [2005] NSWADT 233 .... 6.50

Ormonde v NSW National Parks & Wildlife Service (No 2) [2004] NSWADT 253 .... 8.13

PN v Department of Education and Training [2006] NSWADT 122 .... 5.41-5.42

Police Force of Western Australia v Ayton [1999] WASCA 233 .... 5.49

Raciti v Hughes (unreported, New South Wales Supreme Court, Young J, 3667 of 1995, 19 October 1995) 5.102

Re Pasla and Australia Postal Corporation (1990) 20 ALD 407 .... 5.46

SW v Forests New South Wales [2006] NSWADT 74 .... 5.45

Taciak v Commissioner of Australian Federal Police (1995) 131 ALR 319 .... 5.6

Vice-Chancellor, Macquarie University v FM [2005] NSWCA 192 .... 5.46-5.47, 6.27

Y v Director General, Department of Education [2001] NSWADT 149 .... 5.40, 5.43

YK v Commissioner of Police, New South Wales Police [2008] NSWADT 81 .... 5.64-5.66

TABLE OF LEGISLATION

Legislation in addition to the Privacy and Personal Information Protection Act 1998 (NSW) and the Health Records and Information Privacy Act 2002 (NSW).

Commonwealth

Australian Capital Territory Government Service (Consequential Provisions) Act 1994 .... 2.6

Australian Passports Act 2005 .... 2.27

Australian Postal Corporation Act 1989 .... 2.28

Census and Statistics Act 1905 .... 2.27

Commonwealth Electoral Act 1918 .... 2.27

Constitution Act 5.99

Copyright Act 1968 .... 3.60, 5.7

Corporations Act 2001 .... 2.27, 3.12, 3.15

Data-matching Program (Assistance and Tax) Act 1990 .... 2.27

Freedom of Information Act 1982 .... 2.19, 2.28

Income Tax Assessment Act 1936 .... 2.27

Migration Act 1958 .... 2.27

Privacy (Private Sector) Regulations 2001 .... 5.73

Privacy Act 1988........1.5, 1.6, 1.11, 1.24, Chapter 2, 3.3, 3.15, 3.56, 3.60, 4.7, 4.20, 4.22, 4.26, 4.32, 4.38, 4.39, 4.45, 4.48,

Privacy Amendment (Private Sector) Act 2000 ..... 2.11, 4.26, 5.73

Taxation Administration Act 1953 .... 2.27

Telecommunications (Interception and Access) Act 1979 .... 2.28

Telecommunications (Interception) Act 1979 .... 3.13

Telecommunications Act 1997 .... 5.100

Workplace Relations Act 1996 .... 3.93

Workplace Relations Amendment (Transition to Forward with Fairness) Act 2008 .... 3.93

New South Wales

Administrative Decisions Tribunal Act 1997 .... 7.31, 7.33, 7.36, 7.38

Adoption Act 2000 .... 3.13, 5.7, 5.29

Children and Young Persons (Care and Protection) Act 1998 .... 1.17, 1.18

Conveyancing Act 1919 .... 3.31

Crimes (Forensic Procedures) Act 2000 .... 3.2, 5.95

Crimes Act 1900 .... 5.102

Freedom of Information Act 1989 .... 1.3, 1.29, 3.2, 3.13, 3.29, 5.24, 5.25, 5.28, 5.29, 6.33, 6.34, 6.35, 7.40, 8.2, 8.4, 8.5, 8.7, 8.8-8.28.

Genetic Privacy and Non-discrimination Bill 1998 .... 5.95

Health Service Act 1997 .... 5.55

Human Tissue Act 1983 .... 5.95

Interpretation Act 1987 .... 4.25, 5.52, 7.16, 7.19

Interpretation Amendment Act 2006 .... 5.52

Landlord and Tenant (Amendment) Act 1948 .... 5.52

Law Enforcement (Controlled Operations) Act 1997 .... 3.13

Listening Devices Act 1994 .... 3.2, 3.93

Local Government Act 1993 .... 1.3, 1.29, 3.2, 3.29, 8.2-8.4, 8.29-8.31, 8.33, 8.36

Ombudsman Act 1974 .... 7.9

Police Act 1990 .... 3.13, 5.30

Privacy and Personal Information Protection (Transitional) Regulation 1999 .... 3.7

Privacy and Personal Information Protection Regulation 2000 .... 3.7

Privacy and Personal Information Protection Regulation 2005 .... 3.31, 4.12

Privacy Committee Act 1975 .... 3.3, 3.5

Protected Disclosures Act 1994 .... 3.13

Public Finance and Audit Act 1983 .... 5.51, 5.53

Public Health Act 1991 .... 4.40

Real Property Act 1900 .... 3.31

State Owned Corporations Act 1989 .... 5.70, 5.74, 5.75

State Records Act 1998 . 1.3, 1.29, 3.2, 3.60, 7.8, 8.2-8.5, 8.38-8.41

Water Management Act 2000 .... 3.31

Witness Protection Act 1995 .... 3.13

Workplace Surveillance Act 2005 .... 3.2, 5.102

Northern Territory

Information Act 2002 .... 4.25

Tasmania

Personal Information Protection Act 2004 .... 6.67

Victoria

Health Records Act 2001 .... 4.25, 4.32, 4.44

Information Privacy Act 2000 .... 4.22, 4.27, 4.28, 4.29, 5.81

Other

Data Protection Act 1998 (UK) 6.41

Personal Information Protection and Electronic Documents Act 2000 (Canada) 6.41

Bibliography

Australia, House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000)

Australian Law Reform Commission, *Essentially Yours*, (Report 96, 2003)

Australian Law Reform Commission, *Review of Privacy* (Issues Paper 31, 2006)

Australian Law Reform Commission, *Review of Privacy* (Discussion Paper 72, 2007)

Johnston A, *PPIPA in Practice: An Annotated Guide to the Privacy and Personal Information Protection Act 1998* (*NSW)* (2007)

Morison W L, *Report on the Law of Privacy* (No 170, Parliament of New South Wales, 1973)

National Health and Medical Research Council, *Submission to the Review by the Federal Privacy Commissioner of the Private Sector Provisions of the Privacy Act 1988* (Cth) (10 December 2004)

New South Wales Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly)

New South Wales Government, *Response to the Report on the Statutory Review of the Privacy and Personal Information Protection Act 1998*

New South Wales Law Reform Commission, *Guaranteeing Someone Else's Debts* (Report 107, 2006)

New South Wales Law Reform Commission, *Invasion of Privacy* (Consultation Paper 1, 2007)

New South Wales Law Reform Commission, *Surveillance: An Interim Report* (Report 98, 2001)

New South Wales Law Reform Commission, *Surveillance: Final Report* (Report 108, 2005)

New South Wales Ministerial Advisory Committee on Privacy and Health Information, *Panacea or Placebo? Report to the New South Wales Minister for Health* (2000)

Office of the New South Wales Privacy Commissioner, *Annual Report 2005-06* (2006)

Office of the New South Wales Privacy Commissioner, *Protocol for the Handling of Complaints by Privacy NSW* (22 July 2002, revised July 2006)

Office of the Privacy Commissioner, *Getting in on the Act: The Review of Private Sector Provisions of the Privacy Act 1988* (2005)

Paterson M, *Freedom of Information and Privacy in Australia* (Butterworths, 2005)

Prosser W L, "Privacy" (1960) *California Law Review* 48

Senate Legal and Constitutional References Committee, Parliament of Australia, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005)

Solove D J, "A Taxonomy of Privacy" (2006) 154 *University of Pennsylvania Law Review* 477

United States Department of Health and Human Services, *Unique Health Identifier for Individuals: A White Paper* (1998)