



NSW LAW REFORM COMMISSION

Report 127

# Protecting Privacy in New South Wales

May 2010

© New South Wales Law Reform Commission, Sydney, 2010

## Copyright permissions

This publication may be copied, distributed, displayed, downloaded and otherwise freely dealt with for any personal or non-commercial purpose, on condition that proper acknowledgment is included on all uses.

However, you must obtain permission from the NSW Law Reform Commission if you wish to:

- charge others for access to the publication (other than at cost);
- include all or part of the publication in advertising or a product for sale;  
or
- modify the publication.

## Disclaimer

While this publication has been formulated with due care, the NSW Law Reform Commission does not warrant or represent that it is free from errors or omission, or that it is exhaustive.

This publication deals with the law at the time it was first published and may not necessarily represent the current law.

Readers are responsible for making their own assessment of this publication and should verify all relevant representations, statements and information with their own professional advisers.

## Other publication formats

The NSW Law Reform Commission is committed to meeting fully its obligations under State and Commonwealth anti-discrimination legislation to ensure that people with disabilities have full and equal access to our services.

This publication is available in alternative formats. If you require assistance, please contact the Commission (*details on back cover*).

## Cataloguing-in-publication

Cataloguing-in-publication data is available from the National Library of Australia.

ISSN: 1030-0244 (report) ISBN: 978-0-7347-2647-6 (pbk.)

## Letter to the Attorney General

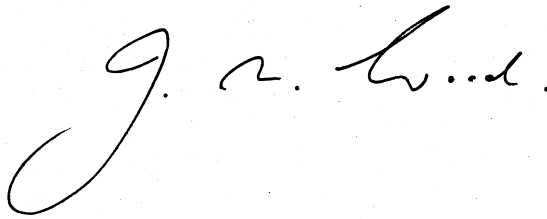
To the Hon John Hatzistergos, MLC  
Attorney General for New South Wales

Dear Attorney

### **Report 127: Protecting Privacy in New South Wales**

We make this Report pursuant to the reference to this Commission received April 2006.

This is the final report in the Privacy reference.

A handwritten signature in black ink, appearing to read 'J. Wood', is centered on the page. The signature is written in a cursive style with a large initial 'J' and a period after the name.

The Hon James Wood AO QC  
Chairperson

May 2010



## Table of Contents

Terms of Reference .....	xi
Participants .....	xiii
LIST OF RECOMMENDATIONS .....	xv
EXECUTIVE SUMMARY .....	xxxv
Scope of privacy legislation.....	xxxv
Exemptions .....	xxxvi
Enforcement.....	xxxvii
<b>1. Introduction .....</b>	<b>1</b>
THIS REPORT .....	2
Background to the report .....	2
The approach of this report.....	3
THE CONTEXT OF THIS REPORT .....	4
The UPPs.....	4
Health information privacy.....	5
The Privacy Commissioner .....	8
THE FORM OF PRIVACY LEGISLATION IN NSW.....	8
AN OBJECTS CLAUSE.....	9
The ALRC's recommendation.....	11
The Commission's View.....	12
<b>2. Public sector agencies .....</b>	<b>15</b>
INTRODUCTION .....	16
CURRENT DEFINITIONS .....	16
Bodies established for a "public purpose" or a public authority established by or under an enactment.....	18
GOVERNMENT BUSINESS ENTERPRISES .....	23
State owned corporations .....	24
Statutory corporations.....	26
Wholly owned subsidiaries.....	27
BODIES ESTABLISHED OTHERWISE THAN BY OR UNDER AN ENACTMENT.....	28
PUBLIC OFFICES.....	30
GOVERNMENT CONTRACTORS .....	31
Liability.....	32
The Commission's view .....	35
MINISTERS.....	36
IDENTIFYING THE RELEVANT AGENCY.....	37
<b>3. Consent .....</b>	<b>41</b>
INTRODUCTION .....	42
CONSENT IN NSW PRIVACY LAW.....	42
What relevance is consent to privacy law? .....	42
The current framework.....	43
The elements of consent.....	46
The approach of the ALRC .....	49
The Commission's view .....	51

Bundled consent .....	51
Express and implied consent .....	52
THIRD PARTY AGENTS .....	54
Current framework .....	54
Submissions and consultations .....	58
The approach of the ALRC .....	61
The Commission's view .....	64
YOUNG PEOPLE .....	67
Introduction .....	67
Current framework .....	67
Submissions .....	69
The approach of the ALRC .....	69
The Commission's view .....	71
<b>4. Exemptions for lawful non-compliance .....</b>	<b>75</b>
INTRODUCTION .....	76
What the chapters on exemptions cover .....	76
What the chapters do not cover .....	77
The differing approaches in PPIPA, HRIPA and the UPPs .....	77
The Commission's approach .....	78
LAWFUL NON-COMPLIANCE .....	79
The rationale of a lawful non-compliance exemption .....	79
The differing approaches in PPIPA, HRIPA and the UPPs .....	80
PPIPA .....	80
HRIPA and the proposed UPPs .....	82
The Commission's view .....	83
DEFINING "LAW" FOR THE PURPOSES OF THE EXEMPTION .....	85
The Commission's view .....	86
A PARTICULAR PROBLEM: PRELIMINARY INQUIRIES .....	89
The Commission's view .....	90
<b>5. Exemptions for law enforcement and investigation .....</b>	<b>93</b>
INTRODUCTION .....	94
GENERAL EXEMPTIONS RELATING TO LAW ENFORCEMENT AND INVESTIGATION .....	94
Legislative provisions .....	94
Issues raised by s 23 of PPIPA .....	96
Issues raised by s 24 of PPIPA .....	98
Law enforcement and investigation under the UPPs .....	102
The Commission's view .....	111
EXEMPTIONS FOR PARTICULAR AGENCIES .....	115
Administrative and educative functions .....	115
Under the UPPs .....	117
The Commission's view .....	118

<b>6. Other exemptions .....</b>	<b>121</b>
INTRODUCTION .....	122
COURTS AND TRIBUNALS .....	122
ROYAL COMMISSIONS AND SPECIAL COMMISSIONS .....	125
SECTION 26 OF PPIPA .....	128
Sub-section 26(1).....	129
Sub-section 26(2).....	130
Section 26 and the proposed UPPs .....	131
The Commission's view .....	131
NAMED BODIES .....	132
Under the UPPs .....	133
The Commission's view .....	133
MINISTERS .....	134
The Commission's view .....	135
ADDITIONAL EXEMPTIONS?.....	135
Alternative dispute resolution .....	135
Suitability for appointment or employment as a public sector official .....	136
Part 8A of the Police Act 1990 (NSW) .....	138
<b>7. Regulatory instruments.....</b>	<b>141</b>
INTRODUCTION .....	142
REGULATIONS .....	143
Issues raised by the regulation-making power .....	144
The Commission's view .....	145
PRIVACY CODES OF PRACTICE .....	147
New South Wales .....	148
Commonwealth privacy codes .....	150
Other Australian jurisdictions .....	151
Clarification of the scope of codes of practice.....	152
Issues raised by current NSW privacy codes of practice .....	155
Reasonableness provisions .....	156
Young people and people lacking capacity.....	159
The application of current Part 2, Division 3 exemptions .....	159
Investigation and law enforcement exemptions .....	160
Whether codes constitute a "lawful excuse" .....	160
The interpretive role of the current codes .....	161
The Commission's view .....	162
PUBLIC INTEREST DIRECTIONS.....	165
Issues.....	166
The Commission's view .....	171

<b>8. Public registers</b> .....	<b>175</b>
INTRODUCTION .....	176
DEFINITION OF A "PUBLIC REGISTER" .....	176
REGULATION OF INFORMATION CONTAINED IN PUBLIC REGISTERS ...	179
ISSUES RAISED BY THE PUBLIC REGISTER PROVISIONS.....	181
PUBLIC REGISTER REGULATION IN OTHER JURISDICTIONS .....	182
Victoria .....	182
New Zealand.....	184
Commonwealth .....	185
POSSIBLE METHODS OF PUBLIC REGISTER REGULATION .....	185
UPP regime.....	185
Statute regime.....	188
Concurrent regime .....	188
<b>9. Enforcement mechanisms</b> .....	<b>193</b>
INTRODUCTION .....	194
COMPLAINT RESOLUTION .....	195
Current approach .....	195
How should complaints be resolved?.....	197
Alternative models .....	199
The Commission's view .....	203
DATA BREACH NOTIFICATION .....	207
ALRC proposal.....	207
Difficulties when formulating data breach notification provisions .....	212
The Commission's view .....	213
ROLE OF CRIMINAL LAW .....	215
Are criminal provisions appropriate in privacy legislation?.....	216
Corrupt disclosure.....	217
Issues.....	218
<b>10. The Privacy Commissioner</b> .....	<b>223</b>
INTRODUCTION .....	224
OVERARCHING FUNCTIONS .....	226
MANAGEMENT .....	227
Staff.....	227
Reporting .....	228
RESEARCH AND EDUCATION .....	228
OVERSIGHT AND COMPLIANCE .....	229
Personal information digests.....	230
Privacy management plans.....	231
Audit powers .....	231
INVESTIGATION AND ENFORCEMENT .....	232
Complaints handling .....	234
Own motion investigations .....	235
Injunctions.....	237
Standing.....	238
LEGISLATION AND POLICY .....	238
Reports to Parliament .....	241



Reporting .....	242
OFFENCES AND LIABILITIES.....	243
Intimidation and threats.....	243
<b>11. Investigation and complaints handling.....</b>	<b>247</b>
INTRODUCTION .....	248
INVESTIGATION.....	248
Meaning of “person” .....	249
Extension of investigative powers .....	257
COMPLAINTS .....	258
Third party complaints.....	258
Violation or interference with privacy .....	260
Preliminary assessment.....	262
Referral.....	263
Dealing with a complaint .....	264
Conciliation .....	265
Reporting .....	267
Representative complaints.....	269
ENFORCEABLE REMEDIES .....	270
<b>12. Internal and external review.....</b>	<b>271</b>
INTRODUCTION .....	272
APPLICATION.....	272
INTERNAL REVIEW.....	272
“Person aggrieved” .....	274
“Conduct” .....	274
The role of the Privacy Commissioner .....	275
Time limits – applicant .....	276
Time limits – agencies .....	277
EXTERNAL REVIEW .....	278
Jurisdiction .....	278
Time limits.....	282
Tribunal orders.....	285
The role of the Privacy Commissioner .....	288
<b>Appendices .....</b>	<b>293</b>
Appendix A: Comparative table of definitions of public sector agency.....	293
Appendix B: Analysis of privacy codes of practice.....	299
Appendix C: Analysis of public interest directions.....	309
Appendix D: Submissions and consultations .....	315
Appendix E: Preliminary submissions.....	317
<b>Tables .....</b>	<b>319</b>
Table of cases.....	320
Table of legislation .....	324



## 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.

By letter received on 1 June 2009, the Attorney General, the Hon J Hatzistergos issued the following additional terms of reference.

Pursuant to section 10 of the *Law Reform Commission Act 1967* (NSW), the Law Reform Commission is also to inquire and report on the legislation and policies governing the handling of access applications for personal information of persons other than the applicant under the *Freedom of Information Act 1989* (or any successor legislation).

In undertaking this review, the Commission is to consider in particular:

- The adequacy of the *Freedom of Information Act 1989* (and any successor legislation) concerning the handling of access applications for personal information in ensuring effective protection of individuals' privacy.
- The adequacy of existing policies, and whether any new policies should be recommended, for the handling of access applications for personal information of persons other than the applicant.
- The circumstances in which agencies should refuse to provide access to personal information of persons other than the applicant on public interest, including privacy, considerations.
- The extent to which public interest, including privacy, considerations against disclosure apply in respect of access applications for personal information of public officials.
- The intersection of, and desirability for a consistent legislative approach to, the treatment of personal information under the *Freedom of Information Act 1989* (and any successor legislation) and other legislation that is concerned with the protection of an individual's privacy.
- Any related matters.

The Attorney General subsequently asked the Commission to consider, as part of these terms of reference, the relationship between the Office of the Privacy Commissioner and that of the newly established Information Commissioner.

## Participants

---

### Division Members

The Hon Judge Kevin O'Connor AM

Professor Michael Tilbury (Commissioner in charge until 26 February 2010)

The Hon James Wood AO QC

### Officers of the Commission

Executive Director

Mr Paul McKnight

Legal research and writing

Mr Liam Boyle

Ms Megan Caristo

Mr Yarran Hominh

Ms Alice Lam

Ms Abi Paramaguru

Research assistance

Mr Simon Ward

Librarian

Ms Anna Williams

Desktop Publishing

Mr Terence Stewart



## LIST OF RECOMMENDATIONS

---

### 1. Introduction

#### RECOMMENDATION 1.1 - *see page 8*

---

On the adoption of a uniform scheme to regulate information privacy in Australia, the *Health Records and Information Privacy Act 2002* (NSW) should be repealed. The *Privacy and Personal Information Protection Act 1998* (NSW) should regulate health information when it is dealt with by public sector agencies. Relevant health-specific provisions, including those in the *Health Records and Information Privacy Act 2002* (NSW), should be incorporated into the *Privacy and Personal Information Protection Act 1998* (NSW).

#### RECOMMENDATION 1.2 - *see page 8*

---

Health information privacy in NSW should be the subject of a separate review.

#### RECOMMENDATION 1.3 - *see page 13*

---

The objects of the *Privacy and Personal Information Protection Act 1998* (NSW) should be to:

- (a) recognise that the law must protect the privacy of individuals;
- (b) recognise that the interest in privacy is not absolute, and so to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests;
- (c) promote the responsible and transparent handling of personal information by public sector agencies;
- (d) provide for the appointment, functions and powers of a Privacy Commissioner;
- (e) provide an accessible framework for the resolution of privacy related complaints;

and, if a national regime regulating information privacy (including the UPPs) is adopted in NSW:

- (f) to facilitate nationally consistent regulation of privacy and the handling of personal information.

## 2. Public sector agencies

### RECOMMENDATION 2.1 - see page 27

---

The definition of “public sector agency” in the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to remove the exclusion for “a State owned corporation”.

### RECOMMENDATION 2.2 - see page 27

---

The definition of “public sector agency” in the *Privacy and Personal Information Protection Act 1998* (NSW) should include a body (whether incorporated or not) established or continued for a public purpose by or under the provisions of a NSW enactment, other than:

- (1) an incorporated company or association; or
- (2) a body regulated pursuant to s 6F of the *Privacy Act 1988* (Cth).

### RECOMMENDATION 2.3 - see page 30

---

The definition of “public sector agency” in the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a body established or appointed, otherwise than by or under a NSW enactment, by the Governor or a Minister.

### RECOMMENDATION 2.4 - see page 31

---

The definition of “public sector agency” in the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include:

- (1) an office or a person holding or performing the duties of an office, established by or under, or an appointment made under, a NSW enactment; and
- (2) an office or a person (and any members of his or her staff) holding or performing the duties of an office to which an appointment is made by the Governor, or by a Minister, otherwise than under a NSW enactment.



**RECOMMENDATION 2.5** - see page 36

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to require an agency entering into a contract for the provision of services with a contracted service provider:

- (1) to take contractual measures to ensure that the contracted service provider does not perform an act, or engage in a practice, that would breach the privacy principles if performed or engaged in by the agency; and
- (2) to ensure that the contract does not authorise the contracted service provider to perform or engage in such an act or practice.

**RECOMMENDATION 2.6** - see page 37

The definition of "public sector agency" in the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include NSW Ministers.

**3. Consent****RECOMMENDATION 3.1** - see page 51

The Privacy Commissioner should consult with the Commonwealth Privacy Commissioner to produce guidelines for NSW agencies about what is required of agencies to obtain an individual's consent for the purposes of NSW privacy law. The guidelines should:

- (1) address the factors that agencies should take into account in assessing whether consent has been obtained; and
- (2) provide how consent can be withdrawn.

**RECOMMENDATION 3.2** - see page 52

The Privacy Commissioner should liaise with the Commonwealth Privacy Commissioner to produce guidelines for NSW agencies that include advice on when it is and is not appropriate to use "bundled consent". The advice should be specific to industry sectors and should be formulated in consultation with relevant stakeholders, industry sectors and individuals.

**RECOMMENDATION 3.3** - see page 54

The Privacy Commissioner should liaise with the Commonwealth Privacy Commissioner to produce guidelines for NSW agencies that cover express and implied consent as it applies in various contexts.

**RECOMMENDATION 3.4** - see page 64

Privacy legislation should provide that an agency may establish nominee arrangements. The agency should then deal with an individual's nominee as if the nominee were the individual.

**RECOMMENDATION 3.5** - see page 65

Nominee arrangements in privacy legislation should provide at a minimum that:

- (1) an individual or a substitute decision maker authorised by a federal, State or Territory law can make a nomination;
- (2) the nominee can be an individual or an entity;
- (3) the nominee has a duty to act at all times in the best interests of the individual; and
- (4) the individual, the nominee or the agency can revoke the nomination.

**RECOMMENDATION 3.6** - see page 65

The Privacy Commissioner should liaise with the Commonwealth Privacy Commissioner to develop guidelines on obtaining consent from an individual with a decision-making disability. The Privacy Commissioner should review the *Best Practice Guide: Privacy and People with Decision-making Disabilities* with a view to ensuring consistency with any such guidelines.

**RECOMMENDATION 3.7** - see page 65

If Recommendation 3.6 is adopted, the guidelines produced by the Privacy Commissioner should be broad enough to negate the need for separate directions and codes for agencies that regularly deal with individuals with decision-making disabilities.

**RECOMMENDATION 3.8** - see page 66

The Privacy Commissioner should develop his or her guidelines in light of the report of the Social Issues Committee of the NSW Legislative Council on the provisions for substitute decision-making for people lacking capacity, the Commonwealth Government's response to the recommendations of the Australian Law Reform Commission and the notification statement produced by the Privacy Commissioner and the NSW Trustee and Guardian.

**RECOMMENDATION 3.9** - see page 67

Agencies that regularly handle personal information about adults with limited or no capacity to provide consent should ensure that relevant staff are trained adequately in relation to issues concerning capacity, and in recognising and verifying the authority of third party representatives.

**RECOMMENDATION 3.10** - *see page 71*

Privacy legislation should provide that an agency is to assess the capacity of an individual under the age of 18 to give consent where it is reasonable and practicable to do so.

**RECOMMENDATION 3.11** - *see page 72*

Privacy legislation should provide that where an assessment of capacity is not reasonable or practicable, then an individual aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access.

**RECOMMENDATION 3.12** - *see page 73*

Where a young person is found to lack the capacity to consent to particular medical treatment but can comprehend an obligation of secrecy with respect to health information obtained by the medical practitioner, the fact that he or she consulted the medical practitioner, and what the medical practitioner has learned in the process of assessing competence to consent to that particular treatment, must not be disclosed if the young person:

- (a) expressly objects to the disclosure; or
- (b) gave the information with an expectation that it would not be disclosed.

**RECOMMENDATION 3.13** - *see page 74*

Agencies and organisations that regularly handle the personal information of individuals under the age of 18 should have privacy policies that address how such information is managed and how the agency or organisation will determine the capacity of individuals under the age of 18. Such agencies and organisations should also ensure that relevant staff are trained about issues concerning capacity, including when it is necessary to deal with third parties on behalf of those individuals.

**4. Exemptions for lawful non-compliance****RECOMMENDATION 4.1** - *see page 83*

If the UPPs are adopted in NSW, s 25 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

**RECOMMENDATION 4.2** - see page 84

If the UPPs are not adopted in NSW:

- (1) s 25(b) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed; and
- (2) s 25(a) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to exempt an agency from compliance with a relevant IPP when non-compliance is required or authorised (whether expressly or impliedly) by or under law.

**RECOMMENDATION 4.3** - see page 89

For the purposes of an exemption in privacy legislation referable to non-compliance required or authorised by or under law (as in s 25(a) of the *Privacy and Personal Information Protection Act 1998* (NSW)) "law" should be defined to include:

- NSW law or Commonwealth law;
- an order of a court or tribunal;
- documents that are given the force of law by an Act; and
- common law and equity.

**RECOMMENDATION 4.4** - see page 91

Section 13AA of the *Ombudsman Act 1974* (NSW) should be amended to require or authorise the disclosure of personal information by an agency for the purpose of the Ombudsman's preliminary inquiries.

## 5. Exemptions for law enforcement and investigation

**RECOMMENDATION 5.1** - see page 112

If the UPPs are adopted in NSW:

- (1) s 23 and s 24 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed;
- (2) the definition of "enforcement body" should include the "law enforcement agencies" and "investigative agencies" listed in s 3 of the *Privacy and Personal Information Protection Act 1998* (NSW); and
- (3) the definition of "enforcement body" should include an authority to the extent that it is responsible for administering, or performing a function under:
  - (a) a law that imposes a penalty or sanction; or
  - (b) a prescribed law.

**RECOMMENDATION 5.2** - *see page 113*

If the UPPs are not adopted in NSW:

- (1) s 23 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to replicate the wording of the equivalent exemptions under the *Health Records and Information Protection Act 2002* (NSW); and
- (2) the definition of “law enforcement agency” should include an authority to the extent that it is responsible for administering, or performing a function under:
  - (a) a law that imposes a penalty or sanction; or
  - (b) a prescribed law.

**RECOMMENDATION 5.3** - *see page 115*

If the UPPs are not adopted in NSW:

- (1) s 24 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to mirror the wording of the equivalent provisions in the HPPs; and
- (2) s 24(6) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

**RECOMMENDATION 5.4** - *see page 119*

Section 27 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended by excluding reference to the NSW Police Force.

**RECOMMENDATION 5.5** - *see page 119*

The Privacy Commissioner should develop guidelines on the meaning of “administrative” and “educative” functions that will assist in the interpretation of privacy legislation.

## 6. Other exemptions

**RECOMMENDATION 6.1** - *see page 128*

If the UPPs are adopted in NSW, s 6(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 13 of the *Health Records and Information Privacy Act 2002* (NSW) should be amended to require Royal Commissions or Special Commissions to be subject to UPP 8.1(a).

**RECOMMENDATION 6.2** - see page 128

If the UPPs are not adopted in NSW:

- (1) s 6(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to require Royal Commissions or Special Commissions to be subject to s 12(c) of that Act; and
- (2) s 13 of the *Health Records and Information Privacy Act 2002* (NSW) should be amended to require Royal Commissions or Special Commissions to be subject to HPP 5(1)(c) of that Act.

**RECOMMENDATION 6.3** - see page 132

If the UPPs are adopted in NSW, s 26 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

**RECOMMENDATION 6.4** - see page 132

If the UPPs are not adopted in NSW s 26(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) and HPP 4(4)(d) of the *Health Records and Information Privacy Act 2002* (NSW) should be repealed.

**RECOMMENDATION 6.5** - see page 134

If the UPPs are adopted in NSW, s 28(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) and HPPs 10(3) and 11(3) of the *Health Records and Information Privacy Act 2002* (NSW) should be repealed.

**RECOMMENDATION 6.6** - see page 135

Section 28(3) of the *Privacy and Personal Information Protection Act 1998* (NSW) and HPPs 10(4) and 11(4) of the *Health Records and Information Privacy Act 2002* (NSW) should be amended to apply where the disclosure is reasonably necessary for the Minister or Premier to perform the ministerial functions relating to that portfolio or agency.

**RECOMMENDATION 6.7** - see page 136

If the UPPs are not adopted in NSW, the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that a public sector agency need not comply with s 8, s 17, s 18 and s 19(1) where non-compliance is necessary for the purpose of a confidential alternative dispute resolution process.

**RECOMMENDATION 6.8** - see page 140

The *Privacy and Personal Information Act 1998* (NSW) should include a specific exemption relating to information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990* (NSW).

**7. Regulatory instruments****RECOMMENDATION 7.1** - see page 146

Regulations should be the main method of imposing on agencies different or more specific privacy requirements that are still consistent with the overall purposes of the *Privacy and Personal Information Protection Act 1998* (NSW).

**RECOMMENDATION 7.2** - see page 147

If Recommendation 10 in Report 125 is not adopted, regulations pursuant to the *Privacy and Personal Information Protection Act 1998* (NSW) should be made after consultation with the Privacy Commissioner.

**RECOMMENDATION 7.3** - see page 155

Privacy legislation in NSW should provide that privacy codes of practice cannot derogate from the standards prescribed in privacy legislation, but only increase privacy protection or clarify the operation of privacy principles.

**RECOMMENDATION 7.4** - see page 155

A public consultation requirement, similar to that in Part 3AA of the *Privacy Act 1988* (Cth), should be adopted to increase the accountability and transparency mechanisms in the creation and adoption of privacy codes.

**RECOMMENDATION 7.5** - see page 155

If Recommendation 7.3 is not adopted, a requirement to publish a statement of reasons in relation to the making of privacy codes, similar to s 79 of the *Privacy Act 1988* (Cth) relating to public interest determinations, should be adopted.

**RECOMMENDATION 7.6** - see page 156

If the UPPs are not adopted, the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to encompass the exemptions provided for in the codes of practice.

**RECOMMENDATION 7.7** - *see page 164*

---

If Recommendation 12 of Report 125 is adopted, the creation and amendment of privacy codes of practice should be performed by the Privacy Commissioner with the approval of the Information Commissioner.

**RECOMMENDATION 7.8** - *see page 164*

---

If Recommendation 12 of Report 125 is not adopted, the Privacy Commissioner should make and amend privacy codes of practice.

**RECOMMENDATION 7.9** - *see page 167*

---

If the UPPs are not adopted, the “Direction Relating to the Disclosures of Information by NSW Public Sector Agencies for Research Purposes” should be incorporated as a specific exemption to the collection, notification, use and disclosure IPPs.

**RECOMMENDATION 7.10** - *see page 170*

---

Section 41 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to allow the Privacy Commissioner to make a public interest direction that applies to a class of agency.

**RECOMMENDATION 7.11** - *see page 170*

---

Section 41 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to give the Privacy Commissioner the power to amend an earlier public interest direction.



**RECOMMENDATION 7.12** - see page 173

In relation to public interest directions, s 41 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include:

- (1) A requirement that the public interest in favour of the public interest direction "substantially outweighs" the public interest in adhering to the privacy principles.
- (2) A limit on the duration of a public interest direction to 12 months without consultation, and a final limit of 3 years (including renewals) unless the Privacy Commissioner decides there are exceptional circumstances that warrant extending or renewing the public interest direction.
- (3) A requirement that the Privacy Commissioner, before issuing a public interest direction of a duration longer than 12 months or renewing a direction, accept public submissions and take these submissions into account.
- (4) A requirement that the Privacy Commissioner publish a statement of reasons for any public interest direction.
- (5) That a public interest direction of duration longer than 12 months is a disallowable instrument.

**RECOMMENDATION 7.13** - see page 174

The Privacy Commissioner must ensure that all public interest directions are made publicly available.

**RECOMMENDATION 7.14** - see page 174

The creation and amendment of public interest directions should not require the approval of the Minister.

## 8. Public registers

**RECOMMENDATION 8.1** - see page 179

If Recommendation 6 of Report 126 is adopted, public registers should be excluded from the proposed definition of "generally available publication".

**RECOMMENDATION 8.2** - see page 179

The definition of "public register" in the *Privacy and Personal Information Protection Act 1998* (NSW) should refer only to registers held by public sector agencies pursuant to an enactment.

**RECOMMENDATION 8.3** - see page 191

Public registers should be subject to the UPPs.

**RECOMMENDATION 8.4** - *see page 191*

If Recommendation 8.3 is adopted, s 59 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

**RECOMMENDATION 8.5** - *see page 191*

If the UPPs are not adopted, public registers should be subject to the IPPs. Section 57 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to say that “a public sector agency must, in administering a public register, so far as is reasonably practicable not perform an act or engage in a practice that would contravene an IPP in respect of information collected, held, managed, used, disclosed or transferred by it in connection with the administration of the public register”.

**RECOMMENDATION 8.6** - *see page 192*

If the UPPs are not adopted, s 59 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that the requirements of the law under which the public register concerned is established prevail to the extent of any inconsistency with the *Privacy and Personal Information Protection Act 1998* (NSW).

**RECOMMENDATION 8.7** - *see page 192*

A review should be undertaken of the establishing statutes of all public registers in order to establish their purpose and proposed form of regulation.

## 9. Enforcement mechanisms

**RECOMMENDATION 9.1** - *see page 207*

Where a public sector agency has allegedly contravened an applicable IPP, privacy code of practice, public register provision, or proposed data breach notification provision, and the Privacy Commissioner notifies the complainant that conciliation has failed, the complainant should be able to apply to the Administrative Decisions Tribunal for external review of the agency's conduct.

**RECOMMENDATION 9.2** - see page 214

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a new Part on data breach notification, that provides as follows:

- (1) An agency is required to notify the Privacy Commissioner and affected individuals when personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.
- (2) In determining whether the acquisition may give rise to a real risk of serious harm to any affected individual, the following factors should be taken into account:
  - (i) whether the personal information was encrypted adequately; and
  - (ii) whether the personal information was acquired in good faith by an employee or agent of the agency where the agency was otherwise acting for a purpose permitted by the *Privacy and Personal Information Protection Act 1998* (NSW) (provided that the personal information is not used or subject to further unauthorised disclosure).
- (3) An agency is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.
- (4) Data breach notification provisions should be enforced in the same manner as an IPP under the *Privacy and Personal Information Protection Act 1998* (NSW).

**RECOMMENDATION 9.3** - see page 220

The Privacy Commissioner and agencies should be under a duty to refer any suspected offences arising under privacy legislation to NSW Police or the Director of Public Prosecutions.

**RECOMMENDATION 9.4** - see page 220

Once a referral has been made pursuant to Recommendation 9.3, the investigation of the Privacy Commissioner in relation to alleged criminal conduct must cease. If it is found that there is insufficient evidence to proceed with the criminal charge, the matter should be referred back to the Privacy Commissioner to complete the investigation.

**RECOMMENDATION 9.5** - see page 221

The title of s 62 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be modified to read "Criminal disclosure and use of personal information by public sector officials".

**10. The Privacy Commissioner****RECOMMENDATION 10.1** - see page 227

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to require that the Privacy Commissioner must have regard to the objects of the Act in the performance of his or her functions and the exercise of his or her powers.

**RECOMMENDATION 10.2** - see page 227

If the Office of the Privacy Commissioner is not established according to the model proposed in Report 125, the Privacy Commissioner should be able to engage consultants without the approval of the Minister for the purpose of getting expert assistance.

**RECOMMENDATION 10.3** - see page 231

If UPP 4 is adopted in NSW, s 33 and s 36(2)(e) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

**RECOMMENDATION 10.4** - see page 231

If UPP 4 is adopted in NSW, the Privacy Commissioner should have the function of assisting public sector agencies in creating and implementing Privacy Policies.

**RECOMMENDATION 10.5** - see page 232

The Privacy Commissioner should be empowered to conduct or commission audits of records of personal information maintained by agencies for the purpose of ascertaining whether the records are maintained according to the IPPs or applicable codes of practice.

**RECOMMENDATION 10.6** - see page 235

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to make it clear that the power of the Privacy Commissioner under s 36(2)(k) "to receive, investigate and conciliate complaints about privacy related matters (including conduct to which Part 5 applies)" and the power to receive or make complaints under s 45(1) "about the alleged violation of, or interference with, the privacy of an individual" are two independent sources of power.

**RECOMMENDATION 10.7** - *see page 237*

The Privacy Commissioner should have the power to initiate own motion investigations.

**RECOMMENDATION 10.8** - *see page 237*

The Privacy Commissioner should be able to serve compliance notices on agencies, following an own motion investigation, that specify action that must be taken to ensure compliance with privacy legislation.

**RECOMMENDATION 10.9** - *see page 238*

The Privacy Commissioner should be able to apply to the Supreme Court to obtain an injunction where a person:

- (1) has engaged, is engaged or is proposing to engage in any conduct that constituted, constitutes or would constitute a contravention of privacy legislation; or
- (2) has refused or failed, is refusing or failing, or is proposing to refuse or fail, to do any act or thing that the person is required to do by or under privacy legislation.

**RECOMMENDATION 10.10** - *see page 238*

The Privacy Commissioner should have the power to bring proceedings by way of judicial review in connection with an agency's exercise of a function under privacy legislation.

**RECOMMENDATION 10.11** - *see page 240*

If Recommendations 7.7 or 7.8 are adopted, the general functions of the Privacy Commissioner should include the approval of privacy codes of practice.

**RECOMMENDATION 10.12** - *see page 240*

The general functions of the Privacy Commissioner should include issuing public interest directions.

**RECOMMENDATION 10.13** - *see page 242*

If Recommendation 9 in Report 125 is not adopted, the Privacy Commissioner should be required to report annually to the Minister on the operation of privacy legislation. The Minister must table the report in each House of Parliament as soon as practicable after it has been received.

**RECOMMENDATION 10.14** - *see page 245*

Privacy legislation should provide that it is an offence to use threats, intimidation or misrepresentation to persuade an individual to:

- (1) refrain from making or pursuing a complaint under privacy legislation;
- (2) refrain from making or pursuing an internal or external review application; or
- (3) withdraw a complaint or an internal or external review request.

**RECOMMENDATION 10.15** - *see page 245*

Privacy legislation should provide that it is an offence to use, cause, inflict or procure any violence, punishment, damage, loss or disadvantage to any individual due to that individual:

- (1) making a complaint to the Privacy Commissioner;
- (2) assisting the Privacy Commissioner;
- (3) providing evidence to the Privacy Commissioner; or
- (4) conducting, or assisting in, an internal review.

**RECOMMENDATION 10.16** - *see page 245*

Privacy legislation should provide that it is an offence for an employer to dismiss or prejudice an employee due to the employee assisting the Privacy Commissioner.

## 11. Investigation and complaints handling

**RECOMMENDATION 11.1** - *see page 257*

Sub-sections 37(1), 37(2)(a), 37(2)(b) and 43(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to refer to "any person" rather than "any person or public sector agency".

**RECOMMENDATION 11.2** - *see page 257*

The *Privacy and Personal Information Protection Act 1998* (NSW) should, without limiting the definition of "person" in the *Interpretation Act 1987* (NSW), state that "person" includes a public sector agency.

**RECOMMENDATION 11.3** - *see page 257*

The Privacy Commissioner should be given the power to enter and inspect premises occupied by a public sector agency and inspect any document or thing on the premises.

**RECOMMENDATION 11.4** - *see page 260*

Sub-section 45(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be reworded to clarify that it is not limited to an individual whose privacy has been violated, or a person acting on behalf of that individual.

**RECOMMENDATION 11.5** - *see page 262*

The Privacy Commissioner should issue guidelines to indicate what he or she will take into account when determining whether to deal with a complaint under privacy legislation.

**RECOMMENDATION 11.6** - *see page 263*

The Privacy Commissioner should be able to decide not to deal with a complaint if the complainant has not responded to the Commissioner for a specified period following a request by the Commissioner for a response in relation to the complaint.

**RECOMMENDATION 11.7** - *see page 265*

The Privacy Commissioner should have the power to conduct an inquiry or investigation into any general issue raised by a withdrawn complaint.

**RECOMMENDATION 11.8** - *see page 267*

Where there have been reasonable attempts to conciliate a complaint and the Privacy Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify both parties that conciliation has failed.

**RECOMMENDATION 11.9** - *see page 268*

Section 50 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to state that findings and recommendations can include:

- a finding that, in the opinion of the Privacy Commissioner, there has been a contravention of privacy legislation; and
- matters relating to a conciliation that has been undertaken under s 49.

**RECOMMENDATION 11.10** - *see page 268*

Section 50 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to allow the Commissioner to make a written report of findings and recommendations as a result of any investigation.

**RECOMMENDATION 11.11** - see page 269

Reports made by the Privacy Commissioner under s 50 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be admissible in subsequent external review proceedings relating to the complaint.

**12. Internal and external review****RECOMMENDATION 12.1** - see page 272

Internal and external review under Part 5 of the *Privacy and Personal Information Protection Act 1998* (NSW) should apply to contravention of data breach notification provisions.

**RECOMMENDATION 12.2** - see page 276

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

**RECOMMENDATION 12.3** - see page 277

Sub-section 53(3) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to allow for individuals, in exceptional circumstances, to request internal review of conduct outside the six-month limitation period.

**RECOMMENDATION 12.4** - see page 282

The *Privacy and Personal Information Protection Act 1998* (NSW) should include a note stating that application to the Administrative Decisions Tribunal, following an internal review, is heard in the Tribunal's "review" jurisdiction.

**RECOMMENDATION 12.5** - see page 284

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a limitation period for application to the Administrative Decisions Tribunal for review so that an application for external review of a complaint must be made within 60 days after:

- (1) the complainant is notified by the Privacy Commissioner that the conciliation has failed;
- (2) the applicant receives notification of the findings of an internal review under s 53(8); or
- (3) the agency has failed to notify the applicant of the findings of the review within the prescribed time (74 days).



**RECOMMENDATION 12.6** - *see page 285*

The Administrative Decisions Tribunal should permit out of time requests for review in exceptional circumstances.

**RECOMMENDATION 12.7** - *see page 285*

The Privacy Commissioner or relevant agency should inform all complainants or internal review applicants of any relevant right to review by the Administrative Decisions Tribunal and also the time limits that apply.

**RECOMMENDATION 12.8** - *see page 286*

If Recommendation 9.2 is adopted, the Administrative Decisions Tribunal should be able to make an order requiring a public sector agency to comply with notification requirements in data breach notification provisions.

**RECOMMENDATION 12.9** - *see page 288*

If Recommendation 9.1 is adopted, the orders that can be made by the Administrative Decisions Tribunal subsequent to a complaint to the Privacy Commissioner should be consistent with the orders that can be made under s 55(2) of the *Privacy and Personal Information Protection Act 1998* (NSW).

**RECOMMENDATION 12.10** - *see page 289*

The *Privacy and Personal Information Protection Act 1998* (NSW) should set out the scope of the Privacy Commissioner's role in the Administrative Decisions Tribunal. This should be determined in consultation with the Privacy Commissioner and the President of the Administrative Decisions Tribunal. The primary role should be to assist in matters of statutory interpretation and privacy practice in NSW.

**RECOMMENDATION 12.11** - *see page 290*

---

Section 56 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include provisions that the Privacy Commissioner:

- (1) is to be notified by the Tribunal of any application made to it under s 56; and
- (2) has a right to appear and be heard in any proceedings before the Tribunal in relation to a review under s 56.

**RECOMMENDATION 12.12** - *see page 291*

---

If Recommendation 9.1 is adopted, the Privacy Commissioner should have the right to appear and be heard in any proceedings before the Administrative Decisions Tribunal where external review is being conducted subsequent to a complaint to the Privacy Commissioner.

## EXECUTIVE SUMMARY

0.1 This is the fifth and final report in our review of the law of privacy in NSW. The focus of this report is on the extent to which the current legislative regulation of privacy in NSW effectively protects individual privacy. Our 104 recommendations aim to simplify the law as well as remove inconsistency and ensure adequate coverage and enforcement of privacy legislation. In this report we:

- ensure that the legislation is effective both in reaching all public sector agencies in this State (chapter 2), and in protecting individuals in circumstances in which they consent, or appear to consent, to the use of their personal information (chapter 3);
- recommend that exemptions from privacy legislation be simple, reasonable and necessary (chapters 4-8); and
- make recommendations to ensure legislation provides adequate enforcement mechanisms (chapters 9-12).

## SCOPE OF PRIVACY LEGISLATION

0.2 As foreshadowed in Report 123 *Privacy Principles*, where we recommend adopting the Unified Privacy Principles (“UPPs”) to achieve national uniformity, we make a number of recommendations aimed at ensuring clear and consistent coverage of privacy legislation across Australia. In chapter 1, we recommend that the *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”) be repealed and health information, as dealt with by public sector agencies, be regulated under the *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”). This would mean that the *Privacy Act 1988* (Cth) would deal with health information handled in the private sector. We further recommend that health information privacy in NSW should be the subject of a separate review, noting the importance of consistency in the way that health information is dealt with, both between Commonwealth and State jurisdictions, and between the public and private sectors.

0.3 The definition of public sector agency contained in PPIPA needs to be amended to achieve consistency and comprehensiveness in the management of information by public sector agencies. We therefore recommend, in chapter 2, that the definition of public sector agency in PPIPA be amended to accord with that in the *Government Information (Public Access) Act 2009* (NSW) (the “GIPA Act”) and address the gaps in coverage created by the operation of the *Privacy Act 1988* (Cth). Our

recommendations expand the current definition of public sector agency by, for example, bringing in State owned corporations (since many are not currently covered by Commonwealth privacy law). We also recommend that agencies be required to ensure that contracted service providers who hold information on behalf of Government comply with NSW privacy legislation.

0.4 Privacy legislation in many situations requires consent to the handling of an individual's personal information. In chapter 3 we recommend that guidelines be developed to clarify the meaning of "consent" in the context of privacy. PPIPA is generally silent on the issue of capacity and how consent can be provided where, for example, there is an individual with a decision-making disability. We recommend that privacy legislation be amended to provide a framework to:

- help assess capacity as it applies to young people; and
- allow a representative to consent where a person is unable to act themselves.

We also recommend the development of guidelines and the implementation of training to address remaining issues in relation to capacity.

## EXEMPTIONS

0.5 There is a great deal of concern about the operation of the exemptions from privacy legislation. Exemptions are scattered throughout legislation, regulations, privacy codes of practice and public interest directions (PIDs). This makes it difficult for agencies to determine whether a particular act or practice is exempt. The fragmented and confusing exemption mechanisms should be amended to bring some clarity and transparency to the operation of privacy legislation. In chapters 4-7 we recommend that, if the UPPs are adopted, many of the exemptions from privacy legislation as well as those contained in codes of practice and PIDs should be removed because the UPPs already adequately address them. For example, the UPPs allow non-compliance in circumstances associated with law enforcement and investigation, this renders many specific exemptions applicable to law enforcement and investigative agencies in PPIPA redundant. Additionally, the language used in the UPPs is clearer and solves many of the problems associated with the current drafting of exemptions. If the UPPs are not adopted, we recommend a number of amendments to the exemptions in order to:

- promote clarity and create sufficient breadth to allow for necessary agency functions that may otherwise contravene privacy legislation (thereby limiting the need for many existing codes and PIDs); and
- limit exemptions that are unnecessarily broad.

We also recommend the inclusion of new exemptions where appropriate.

0.6 Regulations, codes and PIDs are all used to create exemptions from various privacy principles. The choice between these options is confusing for many agencies and leads to delays and a lack of flexibility in crafting necessary exemptions or clarifications. Further, in some cases, there is a lack of transparency and accountability in the process of creating an exemption. In chapter 7 we recommend a scheme where each method plays a different role:

- Legislative amendment should be used for substantial or permanent exemptions from the privacy principles (wherever possible).
- Regulations should be used to impose different or more specific privacy requirements that are still consistent with the overall purposes of the Act.
- Privacy codes should only be used to interpret or modify the application of the privacy principles, and should not be allowed to derogate from them.
- PIDs should be used only as temporary measures (to decrease the privacy protection afforded by privacy legislation) while longer-term measures are developed.

We also recommend that the Privacy Commissioner should have a larger role to play in the creation and amendment of all regulatory instruments and the entire process should be made more open and accessible.

0.7 In chapter 8 we analyse the current regulatory scheme for public registers and recommend that they should be regulated concurrently by both the privacy principles and the statutes establishing the public registers. We also recommend a simplification of the definition of “public register”.

## ENFORCEMENT

0.8 We make a number of recommendations to encourage compliance with requirements under privacy legislation and make enforcement more

effective. Information Protection Principles in PPIPA are enforced primarily through an agency's internal review of its conduct or decision, or optional conciliation by the Privacy Commissioner. In chapter 9 we recommend extending the framework for enforcement by allowing external review by the ADT where Privacy Commissioner conciliation has failed. If there is an increase in the resources available to the Privacy Commissioner, consideration should be given to providing the Commissioner with the power to issue determinations that are reviewable by the ADT. We also make recommendations to improve the effectiveness of criminal provisions, which have been infrequently used. This includes, for example, a requirement that the Privacy Commissioner and agencies refer suspected criminal conduct under PPIPA to NSW Police or the Director of Public Prosecutions.

0.9 We recommend the inclusion of data security breach notification provisions in NSW legislation. This would require agencies to notify affected individuals and the Privacy Commissioner when an unauthorised person has acquired personal information and the agency or Privacy Commissioner believes that the acquisition gives rise to a real risk of serious harm. This will promote transparency in information-handling practices and may protect compromised personal information from further misuse.

0.10 There is also a need to strengthen the powers of the Privacy Commissioner, in particular to enhance the Commissioner's ability to deal with systemic issues. We therefore recommend, in chapter 10, that the Privacy Commissioner be given the power to initiate audits and own motion investigations. In chapters 11-12 we also make a number of recommendations to clarify enforcement provisions to remove ambiguity and address procedural gaps, for example, by including time limits for applying to the ADT for review of conduct.

# 1. **Introduction**

- This report
- The context of this report
- The form of privacy legislation in NSW
- An objects clause

## THIS REPORT

1.1 This is the final report in our review of the law of privacy in NSW.

### Background to the report

1.2 In April 2006 the then Attorney General, the Hon R J Debus, issued the terms of reference for this review.<sup>1</sup> They required us to report generally on whether existing legislation in NSW provides an effective framework for the protection of the privacy of an individual. In doing so, we were to consider the desirability of privacy protection being uniform across Australia and across key legislative instruments dealing with privacy in NSW. We were also required to report on the desirability of introducing a statutory tort of invasion of privacy in NSW.

1.3 Our terms of reference envisaged that, in carrying out our inquiry, we would liaise with the Australian Law Reform Commission (“ALRC”), which was then conducting a review of the *Privacy Act 1988* (Cth). The ALRC reported in May 2008.<sup>2</sup>

1.4 We agreed with the ALRC that we would concentrate the initial focus of our inquiry on the desirability of introducing a statutory cause of action for invasion of privacy in NSW. We issued a consultation paper dealing with this topic in May 2007,<sup>3</sup> and a final report in April 2009.<sup>4</sup>

1.5 We issued a Consultation Paper (“CP 3”) dealing with the legislative regulation of privacy in NSW in June 2008.<sup>5</sup> The first report to flow from CP 3 was issued in August 2009.<sup>6</sup> That report, *Privacy Principles*, deals with the principles that ought to govern primarily the collection, storage, use, disclosure, security and quality of data held by government agencies and, in the case of health information, by organisations. The report also considers the principles relating to the

- 
1. The terms of reference are set out on p xi .
  2. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”).
  3. NSW Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007).
  4. NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009).
  5. NSW Law Reform Commission, *Privacy Legislation in New South Wales*, Consultation Paper 3 (2008) (“NSWLRC CP 3”).
  6. NSW Law Reform Commission, *Privacy Principles*, Report 123 (2009) (“NSWLRC Report 123”).



access to, and correction of, such data. With minor modifications, the report adopted the Unified Privacy Principles (“UPPs”) that the ALRC had formulated in its report on privacy.<sup>7</sup>

1.6 In June 2009, the Attorney General, the Hon J Hatzistergos, issued additional terms of reference requiring us, as part of our broader inquiry into privacy, to report on the legislation and policies governing the handling of applications for access to the personal information of people other than the applicant under the *Freedom of Information Act 1989* (NSW) (the “FOI Act”) and any successor legislation (which refers in particular to the *Government Information (Public Access) Act 2009* (NSW) (the “GIPA Act”), which, at the time of writing, is not yet in force).<sup>8</sup> We were also asked to consider the relationship between the Offices of the Privacy Commissioner and the newly established Information Commissioner. We have reported separately on both these issues.<sup>9</sup> The particular focus of the additional terms of reference was the determination of the adequacy of the provisions dealing with access to personal information in the FOI Act and the GIPA Act in ensuring the effective protection of individuals’ privacy.

### The approach of this report

1.7 In this report we return to our principal terms of reference. We draw, as we did in our report on *Privacy Principles*, on issues raised in, and submissions received in response to, CP 3.<sup>10</sup> The focus of this report is on the extent to which the current legislative regulation of privacy in NSW effectively protects individual privacy. Our recommendations aim to simplify the law as well as remove inconsistency and ensure adequate coverage and enforcement of privacy legislation. Our report deals with this from three perspectives:

- First, we consider whether the scope of the legislation is effective both in reaching all public sector agencies in this State (chapter 2), and in protecting individuals in circumstances in which they

---

7. See NSWLRC Report 123, xix-xxxiii.

8. For the additional terms of reference, see p xi-xii

9. See NSW Law Reform Commission, *The Offices of the Information and Privacy Commissioners*, Report 125 (2009) (“NSWLRC Report 125”); NSW Law Reform Commission, *Access to Personal Information*, Report 126 (2010).

10. A list of submissions and consultations appear in Appendix D and Appendix E to this report.

consent, or appear to consent, to the use of their personal information in ways that may interfere with their privacy (chapter 3).

- Secondly, we explore the question whether the many exemptions and exceptions that are found in privacy legislation effectively weaken its force or even render it ineffective (chapters 4-8).
- Thirdly, we examine the effectiveness of the enforcement mechanisms available under the legislation (chapters 9-12).

## THE CONTEXT OF THIS REPORT

1.8 This report differs from previous reports in that it considers the effectiveness of the two principal legislative instruments protecting privacy in NSW, namely, the *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”) and the *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”). However, the future of these Acts is tied up with the future of privacy law in this State, which, at the time of writing, is unclear. In our review of privacy law, we have stressed the desirability of, and the need for, uniform privacy laws in Australia.<sup>11</sup> Uniformity was also a key feature in the reforms of privacy law that the ALRC recommended in its 2008 report.<sup>12</sup> The Australian Government has accepted in principle the need for uniformity of privacy laws in Australia.<sup>13</sup> Our recommendations in this report necessarily take into account the vision of the uniform law that results from these developments. Three particular aspects of that vision require specific comment: the UPPs; health information privacy; and the Office of the NSW Privacy Commissioner.

### The UPPs

1.9 The proposed UPPs comprise principles relating to the collection, storage, handling and disclosure of personal information that are stated at a high level of abstraction. Unlike prescriptive rules, they are designed

---

11. See NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [11.1]-[11.3]; NSWLRC Report 123, [0.10]-[0.13].

12. ALRC Report 108, vol 1, especially ch 3.

13. See Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice* (2009) (“Australian Government First Stage Response to ALRC Report 108”) 21.

both to facilitate their application in diverse areas of law and to ensure their continued relevance in the light of changing circumstances (such as those associated with developing technology) by enunciating the outcomes that are to be achieved by the entities that they regulate.<sup>14</sup> The UPPs form the backbone of the regulation of information privacy in the ALRC's proposed national scheme of regulation that we support.<sup>15</sup> At the time of writing this report, it is impossible to say if and when the UPPs will be translated into legislation at the Commonwealth level, in NSW or nationally, although the Australian Government has given general and in principle support to the UPPs developed by the ALRC as part of a national scheme of regulating information privacy across Australia.<sup>16</sup>

1.10 It is, of course, up to the NSW Government to determine whether or not the UPPs ought to be adopted in privacy legislation in NSW. For the purpose of considering the issues raised in this report, we have made recommendations both on the assumption that the UPPs will be implemented in NSW and on the assumption that they will not. In the latter case, our recommendations are based on reform of the provisions in PPIPA, and, subject to what we have to say in the next section, HRIPA.

## Health information privacy

### *HRIPA in the proposed scheme of national regulation*

1.11 HRIPA regulates the handling of health information in NSW not only by public sector agencies but also by the private sector. The ALRC has recommended that federal privacy legislation cover the field with respect to the private sector.<sup>17</sup> This means that, in the proposed national scheme, HRIPA will be inapplicable to the private sector in NSW. In CP 3 we proposed that, because of this recommendation, NSW privacy legislation should only apply to public sector agencies.<sup>18</sup> The Australian government has accepted the ALRC's recommendation in principle.<sup>19</sup>

### *Submissions*

1.12 All submissions, bar one, generally agreed that NSW privacy legislation should only apply to public sector agencies, provided that

---

14. NSWLRC Report 123, [0.5]-[0.9].

15. See NSWLRC Report 123.

16. See Australian Government First Stage Response to ALRC Report 108.

17. ALRC Report 108, Recommendation 3-1.

18. NSWLRC CP 3, Proposal 3.

19. Australian Government First Stage Response to ALRC Report 108, 21.

national uniformity was indeed achieved.<sup>20</sup> The HIV/AIDS Legal Centre opposed the federalisation of private sector regulation unless a role was retained for informal proceedings in the Administrative Decisions Tribunal, rather than in the Federal Magistrates Court.<sup>21</sup> The Centre did, however, recognise that the ALRC had recommended maintaining a role for NSW adjudicative bodies, particularly in respect of health information.<sup>22</sup> Justice Health opposed the handing over of responsibility for health information in the private sector to the Commonwealth.<sup>23</sup>

### *Repeal of HRIPA*

1.13 In pursuit of the goal of uniform national laws regulating privacy, we favour the repeal of HRIPA for two principal reasons.

1.14 First, the proposed uniform scheme would mean that there would be no need for HRIPA insofar as it applies to the private sector.<sup>24</sup> Health information in the private sector will be dealt with federally under the *Privacy Act 1988* (Cth), by the UPPs<sup>25</sup> and by guidelines.<sup>26</sup> Many of the provisions in HRIPA regulate private bodies.<sup>27</sup> Enforcement of health related privacy complaints against public sector agencies are currently cross-referenced to PPIPA.<sup>28</sup>

1.15 Secondly, we recommend that specific provisions of HRIPA that apply to the regulation of health information by public sector agencies should be incorporated in PPIPA.<sup>29</sup> This would provide one cohesive

---

20. Australian Privacy Foundation, *Submission*, 1-2; Cyberspace Law and Policy Centre, *Submission*, 3; Inner City Legal Centre, *Submission*, 9-10; Business Law Committee of the Law Society of NSW, *Submission*, 3; NSW FOI Privacy Practitioners Network, *Submission*, 1; Public Interest Advocacy Centre, *Submission*, 3-4; Privacy NSW, *Submission*, 2.

21. HIV/AIDS Legal Centre, *Submission*, 7.

22. HIV/AIDS Legal Centre, *Submission*, 7; ALRC Report 108, vol 3, [60.41]-[60.54].

23. NSW Justice Health, *Submission*, 1.

24. NSWLRC Report 123, [0.24]; NSWLRC CP 3, [4.40]; ALRC Report 108, [3.54], Recommendation 3-1.

25. ALRC Report 108, Recommendation 60-1; Australian Government First Stage Response to ALRC Report 108, 129-130.

26. ALRC Report 108, Recommendation 60-3; Australian Government First Stage Response to ALRC Report 108, 129-30.

27. For example, *Health Records and Information Privacy Act 2002* (NSW) pt 4, pt 6.

28. *Health Records and Information Privacy Act 2002* (NSW) s 21.

29. For example, the provisions relating to referral of complaints: *Health Records and Information Privacy Act 2002* (NSW) s 65-67.

source to which public sector agencies can look to for their privacy obligations. We acknowledge that different policy considerations in relation to privacy can apply in the provision of health services, for example, in facilitating the free flow of reliable healthcare information to achieve better health outcomes. The Healthcare Identifiers Bill 2010 (Cth), which is currently before federal Parliament, attempts to do just this by implementing and maintaining a national system that uniquely identifies healthcare providers and individuals.<sup>30</sup> The different policy considerations underpinning health information privacy may require the articulation of separate rules to supplement or modify the application of the UPPs. We do not attempt this exercise in this report. Rather, we recommend that regulation of health information under PPIPA be dealt with in a separate review. We do wish, however, to emphasise the importance of consistency in the way that health information is dealt with, both between federal and State jurisdictions, and between the public and private sectors.

1.16 The majority of submissions agreed that there was no need for two pieces of NSW privacy legislation given that both would apply only to the public sector.<sup>31</sup> Justice Health's opposition to the repeal of HRIPA was based on the grounds that it may lead to inconsistencies between how health information is managed in the public and private sectors. This concern is, however, addressed by the adoption of uniform privacy principles and the inclusion of consistent Commonwealth and State provisions dealing with health information.

---

30. See Parliament of Australia, House of Representatives, *Parliamentary Debates* 10 February 2010, Second Reading Speech, 3 (The Hon J Rixon, Minister for Health and Ageing).

31. Cyberspace Law and Policy Centre, *Submission*, 6; Inner City Legal Centre, *Submission*, 11; Public Interest Advocacy Centre, *Submission*, 3, 10; Business Law Committee of the Law Society of NSW, *Submission*, 3; Privacy NSW, *Submission*, 1, 2, 5. See also NSW Ombudsman, *Submission*, 2.

**RECOMMENDATION 1.1**

On the adoption of a uniform scheme to regulate information privacy in Australia, the *Health Records and Information Privacy Act 2002* (NSW) should be repealed. The *Privacy and Personal Information Protection Act 1998* (NSW) should regulate health information when it is dealt with by public sector agencies. Relevant health-specific provisions, including those in the *Health Records and Information Privacy Act 2002* (NSW), should be incorporated into the *Privacy and Personal Information Protection Act 1998* (NSW).

**RECOMMENDATION 1.2**

Health information privacy in NSW should be the subject of a separate review.

**The Privacy Commissioner**

1.17 A number of recommendations in this report concern the functions and powers of the Privacy Commissioner. In our report, *The Offices of the Information and Privacy Commissioners*, we recommend that the Office of the NSW Privacy Commissioner should become a division of the Office of the newly established Information Commissioner.<sup>32</sup> If this recommendation is implemented, a number of the current functions of the Privacy Commissioner will, properly, be performed by the Information Commissioner or with the consent of the Information Commissioner.<sup>33</sup> This needs to be borne in mind in reading the recommendations in this report.

**THE FORM OF PRIVACY LEGISLATION IN NSW**

1.18 CP 3 drew attention to the poor structure of PPIPA, in particular to its burying of the Information Protection Principles (“IPPs”) in numbered sections of the Act; the haphazard treatment of exemptions; and its general level of detail and complexity. We also pointed out that, in these respects, HRIPA is more clearly structured and drafted.<sup>34</sup> We proposed that PPIPA should be restructured to locate the IPPs and exemptions to the Act in a schedule to the Act, and to reduce the Act’s level of detail and

32. NSWLRC Report 125, Recommendations 1-4.

33. NSWLRC Report 125, especially ch 5.

34. NSWLRC CP 3, [4.15]-[4.24].

complexity to resemble more closely the structure of HRIPA.<sup>35</sup> Most submissions responding to this proposal supported it.<sup>36</sup>

1.19 If a national scheme of information privacy regulation comes into force, PPIPA will, in any event, have to be completely redrafted. Even if it does not, we would favour a complete revision of the Act so that it is better structured and easier to use.

## AN OBJECTS CLAUSE

1.20 An objects clause sets out the purpose and aims of legislation. It is a useful tool for statutory interpretation in instances of ambiguity or uncertainty. Although an objects clause cannot “control clear statutory language, or command a particular outcome of exercise of discretionary power”,<sup>37</sup> s 33 of the *Interpretation Act 1987* (NSW) provides that a construction that would promote the purpose or object underlying the Act shall be preferred to a construction that would not promote that purpose or object.

1.21 In CP 3 we were of the preliminary view that an objects clause would be a beneficial inclusion in PPIPA.<sup>38</sup> This view accords with the approach taken under HRIPA,<sup>39</sup> similar legislation in Victoria,<sup>40</sup> the Northern Territory,<sup>41</sup> and also, to an extent, at the Commonwealth level.<sup>42</sup>

---

35. NSWLRC CP 3, Proposal 4.

36. Australian Privacy Foundation, *Submission*, 2; Consumer Credit Legal Centre, *Submission*, 1; Cyberspace Law and Policy Centre, *Submission*, 5; Department of Community Services, *Submission*, 2; Inner City Legal Centre, *Submission*, 10-11; NSW Department of Community Services, *Submission*, 2; NSW Department of Primary Industries, *Submission*, 1; NSW FOI/Privacy Practitioners’ Network, *Submission*, 1; Privacy NSW, *Submission*, 2; Public Interest Advocacy Centre, *Submission*, 7-8; State Records Authority of NSW, *Submission*, 3. The NSW Department of Education and Training, *Submission*, 3 expressed concerns about the electronic navigability of items contained in a schedule.

37. *Minister for Urban Affairs and Planning v Rosemount Estates* (1996) 91 LGERA 31, 78 (Cole JA).

38. NSWLRC CP 3, [4.27].

39. *Health Records and Information Privacy Act 2002* (NSW) s 3(1) and s 3(2); noting that this Act provides both a purpose clause and an objects clause.

40. *Information Privacy Act 2000* (Vic) s 1, s 5; noting that this Act provides both a purpose clause and an objects clause. See also *Health Records Act 2001* (Vic) s 6.

41. *Information Act 2002* (NT) s 3. See also the *Information Privacy Bill 2007* (WA) cl 3.

The *Privacy Act 1988* (Cth), however, does not contain an objects clause. The ALRC believed that provisions in principles-based legislation, such as the UPPs, would benefit from an objects clause, which provides a “reference framework” to assist with interpretation.<sup>43</sup> The ALRC recommended that the *Privacy Act 1988* (Cth) should contain an objects clause.<sup>44</sup> The Australian Government has accepted this recommendation in principle.<sup>45</sup>

1.22 Each stakeholder who addressed this issue in response to CP 3 supported the inclusion of an objects clause, noting that it should include a broad statement of the aims and purposes of PPIPA.<sup>46</sup> Most submissions broadly supported the approach taken under the *Information Privacy Act 2000* (Vic),<sup>47</sup> however some reservations were expressed.<sup>48</sup>

1.23 One shared concern was that the objects clause in the *Information Privacy Act 2000* (Vic) did not distinguish between the primary objectives

---

42. *Privacy Amendment (Private Sector) Act 2000* (Cth).

43. ALRC Report 108, vol 1, [5.118].

44. ALRC Report 108, vol 1, Recommendation 5-4.

45. Australian Government First Stage Response to ALRC Report 108, 23.

46. NSW Department of Education and Training, *Submission*; NSW FOI/Privacy Practitioners’ Network, *Submission*; Privacy NSW, *Submission*; Australian Privacy Foundation, *Submission*; Cyberspace Law and Policy Centre, *Submission*; HIV/AIDS, *Submission*; Inner City Legal Centre, *Submission*; Public Interest Advocacy Centre, *Submission*.

47. The main purposes of the *Information Privacy Act 2000* (Vic) are stated in s 1 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. In addition, s 5 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; (c) to promote the responsible and transparent handling of personal information in the public sector.

48. Australian Privacy Foundation, *Submission*, 3; Cyberspace Law and Policy Centre, *Submission*, 5; Public Interest Advocacy Centre, *Submission*, 8.



of the Act (for example, the protection of privacy as a human right), and secondary considerations (for example, the “rights” reflected in the exemptions). Thus it was thought inappropriate to elevate the “free flow of information”<sup>49</sup> to the “status of an objective on a par with the explicitly privacy protective objectives”.<sup>50</sup> In response to criticisms of this nature, the ALRC concluded that an objects clause should recognise the tensions with other interests, and explicitly recognise that privacy is not absolute. It should be an object of the legislation to balance competing rights and interests.<sup>51</sup>

### The ALRC’s recommendation

1.24 The objects clause recommended by the ALRC is similar to the Victorian one. However, there are notable differences in substance and form.<sup>52</sup> Both generally accord with the objects of the legislation articulated in the Second Reading Speech to PPIPA.<sup>53</sup>

1.25 The ALRC recommended that the objects of the *Privacy Act 1988* (Cth) should be to:

- (a) implement, in part, Australia’s obligations at international law in relation to privacy;
- (b) recognise that individuals have a right to privacy and to promote the protection of that right;
- (c) recognise that the right to privacy is not absolute and to provide a framework within which to balance that right with other human rights and to balance the public interest in protecting the privacy of individuals with other public interests;
- (d) provide the basis for nationally consistent regulation of privacy and the handling of personal information;
- (e) promote the responsible and transparent handling of personal information by agencies and organisations;

---

49. *Information Privacy Act 2000* (Vic) s 5(a).

50. Australian Privacy Foundation, *Submission*, 3; Cyberspace Law and Policy Centre, *Submission*, 5.

51. ALRC Report 108, vol 1, [5.122]-[5.126].

52. For example, the *Information Privacy Act 2000* (Vic) s 1(c) specifically addresses a right to correction of personal information.

53. New South Wales, *Parliamentary Debates*, Legislative Council, 17 September 1998, 7598-7599 (The Hon J Shaw, Attorney General).

- (f) facilitate the growth and development of electronic transactions, nationally and internationally, while ensuring respect for the right to privacy;
- (g) establish the Australian Privacy Commission and the position of the Privacy Commissioner; and
- (h) provide an avenue for individuals to seek redress when there has been an alleged interference with their privacy.

### The Commission's View

1.26 We accept that an objects clause would be a beneficial addition to PPIPA. A clear articulation of objectives will assist the Privacy Commissioner in promoting the objectives of privacy legislation.<sup>54</sup> We have had regard to two sources in formulating an objects clause for PPIPA. First, we have taken account of the objects of the statutory cause of action for invasion of privacy that we have recommended and that are expressed in the draft Civil Liability Amendment (Privacy) Bill 2009 (NSW).<sup>55</sup> Secondly, we have considered the ALRC's recommendation, the substance of which we have encapsulated in our recommendation. It is, however, necessary to take into account differences between the federal and State jurisdictions when formulating an objects clause:

- Provisions (a) and (f) of the ALRC recommendation are not suitable for State legislation regulating personal information in the State's public sector. There is no mention of similar objectives in the Second Reading Speech for PPIPA.<sup>56</sup>
- Provisions (c), (g) and (h) require modification to reflect the objects of PPIPA more accurately, while (d) will only be an object if the national regulatory scheme is adopted.
- An object of PPIPA should be to establish the position, functions and powers of the NSW Privacy Commissioner. This accords with

---

54. See NSWLRC Report 125, Recommendation 7.

55. Civil Liability Amendment (Privacy) Bill 2009 (NSW) cl 72, in NSW Law Reform Commission, *Invasion of Privacy* Report 120 (2009) Appendix A.

56. New South Wales, *Parliamentary Debates*, Legislative Council, 17 September 1998, 7598-7599 (The Hon J Shaw, Attorney General).

the Second Reading Speech for PPIPA.<sup>57</sup> Provision (g) should be amended to reflect this.

- The aims, purpose and provisions of PPIPA would be better reflected in (h) by replacing “an avenue for individuals to seek redress when there has been an alleged interference with their privacy” with “an accessible framework for the resolution of privacy related complaints”.<sup>58</sup> This demonstrates that there are multiple accessible paths for redress under NSW privacy legislation.

### RECOMMENDATION 1.3

The objects of the *Privacy and Personal Information Protection Act 1998* (NSW) should be to:

- recognise that the law must protect the privacy of individuals;
- recognise that the interest in privacy is not absolute, and so to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests;
- promote the responsible and transparent handling of personal information by public sector agencies;
- provide for the appointment, functions and powers of a Privacy Commissioner;
- provide an accessible framework for the resolution of privacy related complaints;

and, if a national regime regulating information privacy (including the UPPs) is adopted in NSW:

- to facilitate nationally consistent regulation of privacy and the handling of personal information.

57. New South Wales, *Parliamentary Debates*, Legislative Council, 17 September 1998, 7598-7599: “to establish an office of Privacy Commissioner and to confer on the Privacy Commissioner functions relating to privacy and the protection of personal information” (The Hon J Shaw, Attorney General).

58. This uses the words found in the objects clause under the *Health Records and Information Privacy Act 2002* (NSW) s 3(1)(c).



## 2. **Public sector agencies**

- Introduction
- Current definitions
- Government business enterprises
- Bodies established otherwise than by or under an enactment
- Public offices
- Government contractors
- Ministers
- Identifying the relevant agency

## INTRODUCTION

2.1 It is uncertain which bodies must comply with the requirements of NSW privacy legislation. This uncertainty exists for a number of reasons. First, it is unclear whether bodies established under a NSW enactment or established for a public purpose but not described as a “NSW Government agency” fall within the definition of “public sector agency” under s 3(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”) and s 4(1) of the *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”). Secondly, State owned corporations are expressly excluded from the scope of PPIPA. Thirdly, no provision is made in NSW privacy legislation for the application of privacy governance to government contractors.<sup>1</sup>

2.2 We are of the opinion that the definition of “public sector agency” must be refined to achieve consistency and comprehensiveness in the management of information by public bodies. It must also be amended to accord with the definition of “public sector agency” in the *Government Information (Public Access) Act 2009* (NSW) (the “GIPA Act”) and to address the gaps created by the operation of the *Privacy Act 1988* (Cth). This chapter considers the current definitions of “public sector agency” in PPIPA, HRIPA, the GIPA Act and the *Privacy Act 1988* (Cth) and make recommendations as to how the definition of “public sector agency” can meet these objectives.

## CURRENT DEFINITIONS

2.3 Currently, s 3(1) of PPIPA and s 4(1) of HRIPA, which are identical in all relevant respects, specify that “public sector agency” includes:

- “a government department or the Teaching Service” (item (a));
- “a statutory body representing the Crown” (item (b));
- a declared authority under the *Public Sector Management Act 1988* (NSW) (item (c));<sup>2</sup>

---

1. NSW Law Reform Commission, *Privacy Legislation in NSW*, Consultation Paper 3 (2008) (“NSWLRC CP 3”) [5.51]-[5.55], [5.70]-[5.84].

2. The *Public Sector Management Act 1988* (NSW) sch 3 sets out “declared authorities”, including Cobar Water Board, FSS Trustee Corporation, Greyhound Racing Authority (NSW), Harness Racing NSW, Home Care Service of NSW, Pacific Power, Roads and Traffic Authority of NSW, SAS Trustee

- certain entities ascertained by reference to the auditing requirements of the *Public Finance and Audit Act 1983* (NSW) (item (d));
- the NSW Police Force (item (e));
- a local government authority (item (f)); and
- a person or body that provides data services on behalf of a public sector agency or that receives funding from any such body in connection with providing data services and is prescribed by the regulations for the purposes of the definition of public sector agency (item (g)).<sup>3</sup>

2.4 We raised the concern in CP 3 that the list of agencies included in the definition of “public sector agency” was unduly narrow.<sup>4</sup> Under the *Privacy Act 1988* (Cth), “State and Territory authorities” are not agencies or organisations for the purposes of the Commonwealth privacy scheme.<sup>5</sup> Thus, they are exempt from the operation of the Act, unless they are brought into the regime by regulation.<sup>6</sup> Under s 6C(3) of the *Privacy Act 1988* (Cth), State and Territory authorities are defined broadly to encompass:

- a State or Territory Minister;
- a Department of a State or Territory;
- a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a law of a State or Territory;

---

Corporation, State Rail Authority of NSW, State Transit Authority of NSW, Sustainable Energy Development Authority, Sydney Organising Committee for the Olympic Games, TAFE Commission, Waterways Authority, Zoological Parks Board of NSW. The *Public Sector Management Act 1988* (NSW) was repealed the *Public Sector Employment And Management Act 2002* (NSW) s 165. However, sch 4 of the repealing Act states that “a reference to a declared authority under or within the meaning of former Act is to be read as a reference to a declared authority to which Part 6.4 of this Act applies”.

3. As at February 2010, no persons or bodies have been prescribed by the regulations: see *Health Records and Information Privacy Regulation 2006* (NSW) and *Privacy and Personal Information Protection Regulation 2005* (NSW).
4. NSWLRC CP 3, [5.51]-[5.55], [5.70]-[5.84].
5. See *Privacy Act 1988* (Cth) s 6C.
6. See *Privacy Act 1988* (Cth) s 6F.

- a body established or appointed (otherwise than by or under a law of a State or Territory) by a Governor of a State or a State or Territory Minister;
- a person holding or performing the duties of an office established by or under, or an appointment made under, a law of a State or Territory (other than the office of head of a State or Territory Department); or
- a person holding or performing the duties of an appointment made (otherwise than under a law of a State or Territory) by a Governor of a State or a State or Territory Minister or a State or Territory court.

The definition of “public sector agency” in PPIPA and HRIPA is narrower than the exemption contained in the Commonwealth privacy scheme for State and Territory authorities. The disparity represents a gap in privacy regulation in NSW in that State bodies which do not satisfy the definitions under PPIPA and HRIPA but do satisfy the “State authority” exemption in the *Privacy Act 1988* (Cth) fall outside both the Commonwealth and the State privacy regimes.<sup>7</sup>

2.5 Other entities that potentially fall through the gaps include State Ministers and bodies and persons appointed otherwise than by or under a NSW enactment.<sup>8</sup> The GIPA Act contains a broader definition of “agency” than either PPIPA or HRIPA,<sup>9</sup> which suggests that, to ensure consistency and comprehensiveness in the management of information by public bodies, these omissions may need to be reconsidered.

### **Bodies established for a “public purpose” or a public authority established by or under an enactment**

2.6 In CP 3, we expressed the concern that because the reference in subsection (b) to “a statutory body representing the Crown” appears to be limited to those bodies that are expressly declared to be such by the statute creating its existence,<sup>10</sup> or declared to be a NSW government

---

7. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”) vol 2, ch 38.

8. *Privacy Act 1988* (Cth) s 6C(3)(d) and s 6C(3)(f).

9. *Government Information (Public Access) Act 2009* (NSW) s 4(1).

10. See *McNamara v Consumer Trader and Tenancy Tribunal* (2005) 221 CLR 646.



agency,<sup>11</sup> it is difficult to ascertain whether a body established for a public purpose by or under legislation but falling outside items (a), (b), (c), (e), (f) or (g) is intended to be a public sector agency.<sup>12</sup>

2.7 The *Public Finance and Audit Act 1983* (NSW) imposes certain accounting requirements on “authorities”. An authority is defined in s 4 of that Act to include “statutory authorities”. Schedule 2 to that Act provides an extensive list of “statutory authorities”, including many entities that may not fall within any of the other limbs of the definition of “public sector agency”.

2.8 It seems that this definition does not cover some bodies. For example, the National Trust of Australia (NSW)<sup>13</sup> and the Nature Conservation Trust of NSW<sup>14</sup> do not fall within the definition of public sector agency, as they are not “statutory bodies representing the Crown” nor are they audited pursuant to the *Public Finance and Audit Act 1983* (NSW).<sup>15</sup> Both bodies would appear to be excluded from the ambit of the *Privacy Act 1988* (Cth) as bodies “established or appointed for a public purpose by or under a law of a State”.<sup>16</sup>

2.9 This method of defining “public sector agency” by reference to lists in other legislation does not ensure comprehensive coverage by privacy legislation of public sector activity.<sup>17</sup> Accordingly, we see merit in

---

11. *Interpretation Act 1987* (NSW) s 13A provides that if an Act provides that a body is a NSW Government agency, or a statutory body representing the Crown, the body has the status, privileges and immunities of the Crown.

12. NSWLRC CP 3, [5.51]-[5.55].

13. Established by the *National Trust of Australia (New South Wales) Act 1990* (NSW) s 4.

14. Established by the *Nature Conservation Trust Act 2001* (NSW) s 9.

15. The definition of “public sector agency”, s 3(1) item (d), includes “a person or body a person or body in relation to whom, or to whose functions, an account is kept of administration or working expenses, if the account: (i) is part of the accounts prepared under the *Public Finance and Audit Act 1983*, or (ii) is required by or under any Act to be audited by the Auditor-General, or (iii) is an account with respect to which the Auditor-General has powers under any law, or (iv) is an account with respect to which the Auditor-General may exercise powers under a law relating to the audit of accounts if requested to do so by a Minister of the Crown”.

16. *Privacy Act 1988* (Cth) s 6C(3)(a).

17. For example, courts and tribunals are subject to the requirements of PPIPA because they, as part of the Department of Justice and Attorney General, are

including a more general test by which the definition of “public sector agency” under PPIPA and HRIPA can be ascertained.

2.10 In CP 3 we proposed that the definition of a “public sector agency” be amended to “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”.<sup>18</sup> In respect of HRIPA, the proposed amendment would also include the words “or an affiliated health organisation” in each alternative formulation, to cover those private benevolent organisations that receive 100 per cent of their funding from the government.<sup>19</sup>

2.11 All submissions that responded to this issue supported the proposal for a broader definition of “public sector agency”. There was a uniform recognition of the need to ensure that between the *Privacy Act 1988* (Cth) and PPIPA, all public bodies are covered by privacy law and that any reformulated definition should encompass the widest possible range of public bodies.<sup>20</sup> However, of the two alternative definitions proposed in CP 3, the Business Law Committee of the Law Society of NSW supported only the first definition because it was concerned that the second alternative is potentially more restrictive than the first.<sup>21</sup>

2.12 Of the two alternatives, the first formulation is more widely used in Australian privacy legislation. For instance, the GIPA Act defines “public authority” in sch 4, cl 2 to include “a body (whether incorporated or unincorporated) established or continued for a public purpose by or under the provisions of a legislative instrument”.<sup>22</sup> Further, s 6(1) of the

---

audited by the Auditor-General: *Public Finance and Audit Act 1983* (NSW) s 45F(1). However, this seems to be a rather roundabout way of establishing that courts and tribunals are subject to privacy legislation.

18. See NSWLRC CP 3, Issues 20-21.

19. See NSWLRC CP 3, [5.55]. Note, however, that we have recommended the repeal of HRIPA: Recommendation 1.1.

20. Australian Privacy Foundation, *Submission*, 5; Cyberspace Law and Policy Centre, *Submission*, 13; Inner City Legal Centre, *Submission*, 30.

21. Business Law Committee of the Law Society of NSW, *Submission*, 30.

22. “Public authority” is included in the definition of “agency”: *Government Information (Public Access) Act 2009* (NSW) s 4. Note that this definition of public authority does not include “an incorporated company or association (unless declared to be a public authority for the purposes of the provision by a regulation...)”: sch 4 cl 2(3)(a).

*Privacy Act 1988* (Cth), provides that, with certain exceptions, an agency includes “a body ... established or appointed for a public purpose by or under a Commonwealth enactment”<sup>23</sup> and the *Freedom of Information Act 1989* (NSW) circumscribes its application, relevantly, to “a body (whether incorporated or unincorporated) established or continued for a public purpose by or under the provisions of a legislative instrument”.<sup>24</sup> For a comparison of the scope of the definition of “public sector agency” in PPIPA, the *Privacy Act 1988* (Cth) and the GIPA Act, see Appendix A.

2.13 Although historically the notion of “public purposes” had been equated with government and its purposes,<sup>25</sup> it has more recently been construed in the context of privacy and access to information legislation to involve “some purpose for the benefit of the community, or a substantial segment of the community”.<sup>26</sup> The statutory role of the Municipal Association of Victoria in “promoting the efficient carrying out

---

23. *Privacy Act 1988* (Cth) s 6(1).

24. This definition does not include an incorporated company or association: *Freedom of Information Act 1989* (NSW) s 7. Similarly, the *Information Privacy Act 2000* (Vic) s 9(1)(e) and s 9(1)(f) provide that the Act applies to “a body established or appointed for a public purpose by or under an Act”, and “a body established or appointed for a public purpose by the Governor in Council, or by a Minister, otherwise than under an Act”. Likewise, the *Information Privacy Act 2009* (Qld) s 21(1)(a), defines “public authority” as an entity “established for a public purpose by an Act; or ... established by government under an Act for a public purpose, whether or not the public purpose is stated in the Act”. See also the *Freedom of information Act 1982* (Cth) s 4 where “agency” is defined as “a Department or a prescribed authority” and “prescribed authority” is defined as, relevantly “a body corporate, or an unincorporated body, established for a public purpose by, or in accordance with the provisions of, an enactment or an Order-in-Council”.

25. In *Mersey Docks and Harbour Board Trustees v Cameron* (1865) 11 HL Cas 443, 505; 11 ER 1405, 1429 in relation to the rateability of land used for “public purposes”, Lord Westbury stated that these “must be such as are required and created by the government of the country, and are therefore to be deemed part of the use and service of the Crown”. In a later case, *Greig v University of Edinburgh* (1866) LR 1 Sc & D 348, 354, in respect of the same question, Lord Westbury described “public purposes” as “the purposes of the administration of the government of the country”: see also *Municipal Association of Victoria v Victorian Civil and Administrative Tribunal* [2004] VSC 146, [31].

26. *Municipal Association of Victoria v Victorian Civil and Administrative Tribunal* [2004] VSC 146, [39] (Habersberger J). Note also *Worthing v Rowell* (1970) 123 CLR 89, 125, where Windeyer J stated that the words “public purposes” in the Constitution (Cth) s 52 expressed a “large and general idea”.

of municipal government” has been held to be a public purpose,<sup>27</sup> as have been the powers and functions of the Law Society of Queensland,<sup>28</sup> and the Law Society of the Australian Capital Territory.<sup>29</sup> Moreover, the characteristics of a “public authority” have been held to include carrying out “some undertaking of a public nature for the benefit of the community or of some section or geographical division of the community and that it [has] some governmental authority to do so”.<sup>30</sup> The concept of a “public authority” may more narrowly denote that the body in question has authoritative governmental powers of some kind, but as a number of cases suggest, the purpose of a particular body can only be ascertained by examining the range of powers pursuant to which it carries on its activities and thus defines itself.<sup>31</sup>

2.14 In determining whether an entity has been established “for a public purpose”, courts have held that a body would not be established for a public purpose, nor be a “public authority”, if only one or more of the minor purposes or functions can be said to be public and the majority or more important purposes or functions are of a private nature.<sup>32</sup>

2.15 To avoid any uncertainty as to whether the term “established for a public purpose” has a temporal dimension,<sup>33</sup> the GIPA Act states that a

---

27. *Municipal Association of Victoria v Victorian Civil and Administrative Tribunal* [2004] VSC 146.

28. *Queensland Law Society Inc v Albietz* [1996] 2 Qd R 580.

29. *Re Brennan and the Law Society of the Australian Capital Territory* (1984) 6 ALD 428.

30. *Renmark Hotel Inc v Federal Commissioner of Taxation* (1949) 79 CLR 10, 18 (Rich J).

31. *Re Brennan and the Law Society of the Australian Capital Territory* (1984) 6 ALD 428, 439; *Channel 31 Community Educational Television Ltd v Inglis* (2001) 25 WAR 147, [29].

32. *Western Australian Turf Club v Federal Commissioner Of Taxation* (1978) 19 ALR 167, 174. The High Court noted that the possession of some statutory duties or powers is not enough to attract the exemption unless, upon an examination of all its characteristics, the body can be seen in general to conform to the common understanding of a public authority. See also *Re Brennan and the Law Society of the Australian Capital Territory* (1984) 6 ALD 428, [9]; *Municipal Association of Victoria v the Victorian Civil and Administrative Tribunal* [2004] VSC 146, [30].

33. *Municipal Association of Victoria v Victorian Civil and Administrative Tribunal* [2004] VSC 146, [20].

“public authority” is “a body...established or continued for a public purpose by or under the provisions of a legislative instrument”.<sup>34</sup>

2.16 We are of the view that “public sector agency” in the NSW privacy legislation should be redefined to include a “body established or continued for a public purpose” by or under a NSW Act. This insertion would clarify the status under PPIPA and HRIPA of bodies established for a public purpose but not expressly described in legislation as such and include the widest possible range of public bodies. Recommendations 2.1 and 2.2 gives effect to this.

## GOVERNMENT BUSINESS ENTERPRISES

2.17 The position of State and Territory authorities that are government business enterprises (“GBEs”) also represents a potential gap in the coverage of privacy regulation.<sup>35</sup> GBEs are bodies that are principally engaged in commercial activities but are controlled by the Government and have a legal personality separate to a department of government. A State or Territory GBE may be (a) State owned corporations (“SOCs”) under sch 5 of the *State Owned Corporations Act 1989* (NSW); (b) a body corporate established by legislation for a public purpose;<sup>36</sup> or (c) a company established under the Corporations Law in which a State or Territory government has a controlling interest.

2.18 Under the *Privacy Act 1988* (Cth), the definition of “State and Territory authorities” includes SOCs and statutory corporations,<sup>37</sup> but excludes companies incorporated under the *Corporations Act 2001* (Cth).<sup>38</sup> Thus, SOCs and State statutory corporations are exempt from the operation of the Act unless they are brought into the regime by a regulation made under s 6F of the *Privacy Act 1988* (Cth). Section 6F

---

34. Emphasis added. *Government Information (Public Access) Act 2009* (NSW) sch 4 cl 2.

35. See ALRC Report 108, vol 2, [38.28].

36. Statutory corporations are generally not subject to the *Corporations Act 2001* (Cth) because they usually qualify as exempt public authorities within the meaning of s 9: See *Re NSW Grains Board: Smith v Lawrence* (2002) 171 FLR 68.

37. The *Privacy Act 1988* (Cth) s 6C(3)(c) states that “State or Territory authority” means “a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a law of a State or Territory, other than: (i) an incorporated company, society or association...”

38. See ALRC Report 108, vol 2, [26.40].

allows a State or Territory instrumentality to opt into the private sector regime where the State (or Territory) and Minister (in consultation with the Privacy Commissioner) consider that it is appropriate to do so.

### State owned corporations

2.19 PPIPA and HRIPA explicitly exclude SOCs from the definition of “public sector agency”. Currently, there are 21 SOCs listed in sch 5 to the *State Owned Corporations Act 1989* (NSW), including Sydney Ferries, Railcorp, Sydney Water, NSW Lotteries, Landcom, Energy Australia and Integral Energy, which are not regulated at all by PPIPA.<sup>39</sup> At present, only four SOCs have been brought into the Commonwealth privacy regime by the *Privacy (Private Sector) Regulations 2001* (Cth) under s 6F of the *Privacy Act 1988* (Cth).<sup>40</sup> The 21 SOCs are, however, covered under HRIPA in relation to any health information they hold.<sup>41</sup>

2.20 As explained in CP 3, the rationale for excluding SOCs from the scope of PPIPA was the concern that they could be placed at a “competitive disadvantage” with the private sector, which, in 1998, was not regulated by privacy legislation. However, in 2000 the coverage of the *Privacy Act 1988* (Cth) was extended to the private sector and so this rationale is no longer valid. Further, there is no consistency in the coverage of SOCs in the privacy legislation that now prevails. 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), which aims to achieve both business efficacy and social responsibility by having regard to the interests of the community in which it operates.<sup>42</sup>

2.21 The Australian Law Reform Commission (“ALRC”) has expressed concern over the inconsistent coverage of SOCs under State and Territory privacy laws. For example, statutory corporations are covered by privacy legislation in Victoria but not in NSW, while in Tasmania, privacy

---

39. See *State Owned Corporations Act 1989* (NSW) sch 5 for a list of all statutory State owned corporations.

40. Currently, 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 Integral Energy.

41. See NSWLRC CP 3, [5.74].

42. See the *State Owned Corporations Act 1989* (NSW) s 20E(1)(b).

legislation covers “government business enterprises”.<sup>43</sup> As a result, the ALRC noted that the exemption of State and Territory authorities from the operation of the *Privacy Act 1988* (Cth) represented a significant gap in privacy regulation in Australia, and expressed the view that State-owned statutory corporations that compete with other organisations should not have a competitive advantage over those organisations.

2.22 In CP 3, we proposed that all SOCs should be covered by privacy legislation, either by PPIPA or by the *Privacy Act 1988* (Cth), provided there is no duplication of coverage.<sup>44</sup> This proposal was met with broad support by submissions addressing the issue.<sup>45</sup> Both the Public Interest Advocacy Centre and the Inner City Legal Centre were of the view that irrespective of progress on uniformity or national privacy legislation, this matter ought to be dealt with in NSW as a matter of urgency.<sup>46</sup> NSW State Records pointed out that as SOCs are already covered by the two other major Acts relating to information, the *State Records Act 1998* (NSW) and the *Freedom of Information Act 1989* (NSW), the definition ought to be extended under PPIPA to include SOCs to ensure consistency in the management of information.<sup>47</sup>

2.23 Nonetheless, although it was not addressed in submissions, including SOCs within the NSW privacy framework raises the question of whether those SOCs that are primarily engaged in commercial activities

---

43. The *Information Privacy Act 2000* (Vic) applies to “public sector agency” (see s 3). According to s 9(1)(c) a “public sector agency” is a public service body or a public entity within the meaning of the *Public Administration Act 2004* (Vic). Under the *Public Administration Act 2004* (Vic) s 5, public entities include bodies that are established by or under an Act (other than a private Act) or the *Corporations Act*. Under the *Personal Information Protection Act 2004* (Tas) s 3, a public sector body includes a GBE under the *Government Business Enterprises Act 1995* (Tas). See also ALRC Report 108, vol 2 [38.30].

44. See NSWLRC CP 3, Proposal 6 and [5.78].

45. Australian Privacy Foundation, *Submission*, 6; Consumer Credit Legal Centre, *Submission*, 1; Cyberspace Law and Policy Centre, *Submission*, 16; Inner City Legal Centre, *Submission*, 11; NSW Department of Primary Industries, *Submission*, 1; NSW FOI/Privacy Practitioners’ Network, *Submission*, 1; Office of the Privacy Commissioner, *Submission*, 9; Privacy NSW, *Submission*, 3; Public Interest Advocacy Centre, *Submission*, 16; State Records Authority of NSW, *Submission*, 3.

46. Inner City Legal Centre, *Submission*, 12; Public Interest Advocacy Centre, *Submission*, 16.

47. State Records Authority of NSW, *Submission*, 3.

ought to be distinguished from those SOCs whose core functions primarily concern public administration. Should such an amendment be made to the definition of “public sector agency”, it may be appropriate to ensure that SOCs whose functions are primarily commercial are prescribed under s 6F of the *Privacy Act 1988* (Cth), which allows agencies to be treated as organisations. The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) noted that the opt-in provision was designed to allow statutory corporations whose activities are predominantly commercial to “opt-in” to the private sector privacy regime where the State (or Territory) and Minister (in consultation with the Privacy Commissioner) considers it is appropriate to do so.<sup>48</sup>

2.24 We are of the view that the definition of “public sector agency” should be amended, along similar lines to the *Privacy Act 1988* (Cth), to include bodies incorporated by statute. This would encompass SOCs, and those statutory corporations not already caught by the definition of “public sector agency”. The exclusion of SOCs from the definition of “public sector agency” should, therefore, be removed. We also recommend that the NSW government consider making use of s 6F so that privacy obligations for statutory corporations whose activities are predominantly commercial are subject to the same obligations as the rest of the private sector. The definition of “public sector agency” would therefore include SOCs except those SOCs listed in s 6F of the *Privacy Act 1988* (Cth) to ensure that there is no overlap between PPIPA and the *Privacy Act 1988* (Cth).

### Statutory corporations

2.25 Statutory corporations are not expressly included in or excluded from the definition of “public sector agency”, although many are covered because they are “statutory bodies representing the Crown” for the purposes of item (b) of the definition, or because their accounts are subject to the auditing requirements of the *Public Finance and Audit Act 1983* (NSW) under item (d).<sup>49</sup>

---

48. Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) [102].

49. The *Public Finance and Audit Act 1983* (NSW) sch 2 provides a list of “statutory bodies” covered by the Act. See further para 2.7-2.8.



2.26 As all State statutory corporations are excluded from the *Privacy Act 1988* (Cth),<sup>50</sup> we consider that, to ensure comprehensiveness, the definition of “public sector agency” should be framed to include all bodies “whether incorporated or not” where they are established or continued for a public purpose under a NSW law. This would encompass both SOCs and statutory corporations.

#### RECOMMENDATION 2.1

The definition of “public sector agency” in the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to remove the exclusion for “a State owned corporation”.

#### RECOMMENDATION 2.2

The definition of “public sector agency” in the *Privacy and Personal Information Protection Act 1998* (NSW) should include a body (whether incorporated or not) established or continued for a public purpose by or under the provisions of a NSW enactment, other than:

- (1) an incorporated company or association; or
- (2) a body regulated pursuant to s 6F of the *Privacy Act 1988* (Cth).

### Wholly owned subsidiaries

2.27 Since the 1990s, it has been a common practice for government departments and statutory authorities to set up subsidiary companies as a vehicle for conducting some government activities. As these subsidiaries are separate corporate personalities not established by statute, they are governed by the *Corporations Act 2001* (Cth), and hence the National Privacy Principles (“NPPs”). Consequently, a NSW agency will come within the NSW privacy regime but a wholly owned subsidiary of that agency will be governed by the Commonwealth privacy regime. This anomaly may not be of great significance if national uniformity is achieved.

2.28 Even so, there may still be areas where an agency and its wholly owned subsidiary have different privacy obligations, which may lead to

---

50. The *Privacy Act 1988* (Cth) s 6 states that an “agency” includes “a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a law of a State or Territory, other than: (i) an incorporated company, society or association...”

confusion and to an inefficient use of resources. An issue that therefore arises is whether such entities ought to be governed by PPIPA. The definition of “agency” in the GIPA Act expressly extends the NSW access to information regime to a wholly owned subsidiary of the Crown in right of the State or of a public authority.<sup>51</sup> In the interests of consistency between the GIPA Act and PPIPA, there is a strong argument that wholly owned subsidiaries should be included in the definition of “public sector agency” in PPIPA. However, as Commonwealth legislation will prevail against NSW legislation where the two pieces of legislation are inconsistent,<sup>52</sup> it would not be possible to make such a recommendation without necessary amendments being made to the Commonwealth privacy regime.

## BODIES ESTABLISHED OTHERWISE THAN BY OR UNDER AN ENACTMENT

2.29 Under s 6C of the *Privacy Act 1988* (Cth), a body established or appointed otherwise than by or under a law of a State or Territory by a Governor or a State or Territory Minister is also exempted from the Commonwealth privacy regime. The definition of “public sector agency” in PPIPA and HRIPA does not cover these entities unless they fall within item (d), relating to the auditing requirements of the *Public Finance and Audit Act 1983* (NSW). For example, Royal Commissions are not mentioned in the *Public Finance and Audit Act 1983* (NSW) nor is there anything in the *Royal Commissions Act 1923* (NSW) to suggest that Royal Commissions fall within the definition of “public sector agency” or are subject to the requirements of PPIPA.

2.30 Section 6 of PPIPA, which refers explicitly to Royal Commissions, generates uncertainty as it is not clear why the legislature would find it necessary to state that nothing in PPIPA affects the manner in which the “functions” of Royal Commissions are exercised unless the legislature was of the view that Royal Commissions are subject to the requirements in PPIPA. Section 6 allows for the application to Royal Commissions of such of the IPPs as are appropriate in the circumstances.<sup>53</sup> We viewed this as appropriate, given that Royal Commissions can be established for a variety of purposes and can utilise a diversity of processes and

---

51. See *Government Information (Public Access) Act 2009* (NSW) s 4 and sch 4 cl 2(f).

52. See *Constitution* (Cth) s 109.

53. See 6.11-6.17.

procedures. As we have recommended, it is imperative to clarify the status of Royal Commissions with respect to PPIPA.<sup>54</sup>

2.31 The NSW Natural Resources Advisory Council is an independent body established by the NSW Government (reporting to the Minister for Climate Change and the Environment) that is not established by or under a State law and thus is exempted from both the Commonwealth and State privacy regimes. It is desirable that public bodies such as this should be covered by privacy legislation.

2.32 While the GIPA Act does not currently include bodies established or appointed by the Governor or by a Minister, sch 4, cl 2(2) provides that regulations may declare a public authority to be: (a) a body (whether incorporated or unincorporated) established for a public purpose otherwise than by or under the provisions of a legislative instrument; or (b) a body (whether incorporated or unincorporated) that is established by the Governor or by a Minister or that is an incorporated company or association over which a Minister is in a position to exercise direction or control. No such regulations have yet been made.<sup>55</sup> The *Privacy Act 1988* (Cth) expressly extends to a Commonwealth body established or appointed by the Governor General or by a Minister, otherwise than by or under a federal enactment.<sup>56</sup> We are of the view that the definition of “public sector agency” be amended, to include a body established or appointed, otherwise than by or under a NSW enactment, by the Governor or a Minister.

### RECOMMENDATION 2.3

The definition of “public sector agency” in the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a body established or appointed, otherwise than by or under a NSW enactment, by the Governor or a Minister.

54. See Recommendations 6.1-6.2.

55. As at 3 February 2010. Although note that the *Government Information Public Access Act 2009* (NSW) sch 5 is the *Government Information (Public Access) Regulation 2009*, which regulates public access to information held by local authorities.

56. *Privacy Act 1988* (Cth) s 6(1), definition of “agency” item (d).

## PUBLIC OFFICES

2.33 A “public office” generally denotes an office in the public service of the Commonwealth, a State or Territory, or a local government, with the responsibility of carrying out the activities and functions of government.<sup>57</sup> Examples in NSW include the NSW Ombudsman’s Office, the Office for Children, the Office of Fair Trading and Office of the Director of Public Prosecutions.

2.34 Section 6C of the *Privacy Act 1988* (Cth) excludes from the Commonwealth privacy regime a person holding or performing the duties of an office established by or under, or an appointment made under, a law of a State or Territory (other than the office of head of a State or Territory Department); and a person holding or performing the duties of an appointment made (otherwise than under a law of a State or Territory) by a Governor of a State or a State or Territory Minister.<sup>58</sup> The current definition of “public sector agency” in PPIPA and HRIPA would not cover these entities unless they fell into item (d), relating to the auditing requirements of the *Public Finance and Audit Act 1983* (NSW).

2.35 The definition of “agency” in the *Privacy Act 1988* (Cth) explicitly covers a person holding or performing the duties of an office established by or under a Commonwealth enactment as well as a person holding or performing the duties of an appointment, being an appointment made by the Governor General, or by a Minister, otherwise than under a Commonwealth enactment.<sup>59</sup> The definition of “agency” in the GIPA Act includes an office “established or continued for a public purpose” by or under the provisions of a legislative instrument but leaves the regulations to prescribe as a “public office” any other office to which an appointment is made by the Governor or by a Minister.<sup>60</sup>

2.36 We are of the view that the definition of “public sector agency” should be amended to include an “office” established either by or under a NSW enactment or by the Governor or a Minister. We also recommend that this limb of the definition be drafted to make it clear that the NSW

---

57. LexisNexis, *Encyclopaedic Australian Legal Dictionary* (at 3 March 2010).

58. *Privacy Act 1988* (Cth) s 6C(3)(e)-6C(3)(f).

59. *Privacy Act 1988* (Cth) s 6C(3)(e)- 6C(3)(f).

60. *Government Information (Public Access) Act 2009* (NSW) s 4 includes in its definition of “agency”, a “public office”, which is defined in sch 4 cl 3 of the Act.

privacy regime extends not only to the office holder but also to the office as a government entity.

#### RECOMMENDATION 2.4

The definition of “public sector agency” in the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include:

- (1) an office or a person holding or performing the duties of an office, established by or under, or an appointment made under, a NSW enactment; and
- (2) an office or a person (and any members of his or her staff) holding or performing the duties of an office to which an appointment is made by the Governor, or by a Minister, otherwise than under a NSW enactment.

## GOVERNMENT CONTRACTORS

2.37 PPIPA is generally silent on the status of non-government organisations contracted by public sector agencies to provide services to the public. While the definition of “public sector agency” in s 3, item (g) includes a person or body that provides data services on behalf of a public sector agency or that receives funding from any such body in connection with providing data services and is prescribed by the regulations for the purposes of this definition, no persons or bodies have so far been prescribed.<sup>61</sup> Further, the scope of item (g) is limited to a narrow class of entities “providing data services”.

2.38 Contractors and subcontractors to State and Territory authorities are also exempt from the operation of the *Privacy Act 1988* (Cth) where they are acting under a State or Territory contract.<sup>62</sup> Thus, State or Territory government contractors that are otherwise organisations under the *Privacy Act 1988* (Cth), may not be bound by either State or Commonwealth privacy legislation when performing functions under State or Territory contracts<sup>63</sup>. The ALRC has expressed concern that the

61. See *Privacy and Personal Information Protection Regulation 2005* (NSW).

62. *Privacy Act 1988* (Cth) s 7B(5). The Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 (Cth) considered that it was the intention of the Australian Parliament that the acts and practices of State and Territory contractors would be regulated by the relevant State or Territory.

63. For example, all insurers contracted to WorkCover are private and Privacy NSW reports that there are numerous complaints about breaches of privacy by these

absence of consistent regulation for State contractors and the possible imposition of different obligations can create gaps in privacy protection and generate confusion.<sup>64</sup> The ALRC recommended that State and Territory privacy legislation include provisions relating to State and Territory contractors.<sup>65</sup>

## Liability

2.39 Section 4(4) of PPIPA provides that information is “held” by an agency, and is thus subject to the IPPs, if “the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement”. This suggests that where a contracted service provider breaches a provision of PPIPA, the agency that contracted out the services is liable for the breach. This serves as an incentive for the agency to negotiate clauses in the contract so that it can seek indemnity should it be held liable for a breach of privacy legislation due to the conduct of a contracted service provider. Several submissions supported the retention of this provision.<sup>66</sup>

2.40 However, the doctrine of privity of contract means that individuals have no right to enforce the terms of the contract against the outsourcing service provider.<sup>67</sup> This raises the question of whether liability for breach ought to rest on the outsourcing agency and/or the contractor.

2.41 One way of addressing this question is to include the contractor in the definition of “public sector agency”. However, the ALRC concluded that it was unnecessary to clarify whether the outsourcing agency or a contracted service provider is liable for an interference with privacy. This was because liability for the acts or practices of a contractor will depend on the facts of the case, including the terms of the contract. In the ALRC’s view, it was sufficient that the *Privacy Act 1988* (Cth) ensures that

---

insurers. They are not bound by the IPPs and there is no internal review of conduct: See NSWLRC CP 3, [5.80].

64. ALRC Report 108, vol 1, [14.130].

65. ALRC Report 108, vol 1, [14.135].

66. See NSW Law Reform Commission, *Privacy Principles*, Report 123 (2009) (“NSWLRC Report 123”) [8.69]; Australian Privacy Foundation, *Submission*, 6; Cyber Law and Policy Centre, *Submission*, 16; Inner City Legal Centre, *Submission*, 12.

67. See J Rawlings, “Outsourcing under the amended *Privacy Act 1988*” [2001] *Privacy Law and Policy Reporter* 17.

contracting out of government services does not result in a loss of accountability for the handling of personal information.<sup>68</sup>

2.42 In Queensland, the *Information Privacy Act 2009* (Qld) imposes an obligation on an agency entering into a “service agreement” to bind its service providers to comply with the privacy principles, but only if the contracted service provider will deal with personal information for the contracting agency<sup>69</sup> or if the provision of services under the arrangement will involve the transfer of personal information to the contracting agency or the provision of services to a third party for the contracting agency.<sup>70</sup> Sub-section 36(3) of the Act makes it clear that a bound contracted service provider’s compliance may be enforced under the *Information Privacy Act 2009* (Qld).

2.43 Similarly, under the *Information Privacy Act 2000* (Vic), providers of contracted services are bound by the provisions of the Act to the same extent as the agency seeking to outsource one or more functions. The level of obligation will either be the default legislative scheme or an approved code of practice.<sup>71</sup> The Office of the Victorian Privacy Commissioner has acknowledged that one of the difficulties with the Victorian scheme has been the enforceability of provisions that purport to bind a service provider contractually to the *Information Privacy Act 2000* (Vic). Since the Office of the Victorian Privacy Commissioner lacks

---

68. ALRC Report 108, vol 1, [14.123].

69. See *Information Privacy Act 2009* (Qld) s 35(2)(a).

70. See *Information Privacy Act 2009* (Qld) s 35(2)(b)(i)-35(2)(b)(ii). Under s 35(3), the agency is not required to comply with this requirement if the contracted service provider is the recipient of funding from the public sector agency, and is not collecting personal information on behalf of the contracting agency nor the recipient of any personal information from the contracting agency or required to give any personal information it collects in discharging obligations under the contract.

71. *Information Privacy Act 2000* (Vic) s 17(3). Sub-sections 17(2)-(4) ensure that the outsourcing agency remains liable for contravention of IPPs under the Act unless two requirements are satisfied: first, a suitable contract is operating which provides for the contracted service provider to be bound by the privacy principles and any applicable code of practice, and; secondly, that the IPPs or code must be enforceable against the contracted service provider in accordance with the procedures set out in the *Information Privacy Act 2000* (Vic). If information handling obligations are not specified in an outsourcing contract, the outsourcing organisation will be responsible under the Act or to the extent specified in an approved code.

determinative powers, it cannot decide whether the contractual arrangements have effectively passed on responsibility for compliance where there is disagreement between the agency and the contracted service provider on this issue. Accordingly, the Privacy Commissioner can only determine whether the clause passing responsibility is enforceable and whether the outsourcing agency and/or the contractor are liable for any breach.<sup>72</sup>

2.44 The Inner City Legal Centre and the Public Interest Advocacy Centre both submitted that the aggrieved individual ought to be able to take effective action against either or both the contractor and the principal government organisation.<sup>73</sup>

2.45 Section 12 of PPIPA provides that a public sector agency, where it is necessary to give information to a person in connection with the provision of a service to the agency, must do everything reasonably within the power of the agency to prevent unauthorised use or disclosure of that information. The proposed Unified Privacy Principle (“UPP”) 8 (Data Security) does not have a similar provision. In Report 123, we recommended that UPP 8 should be modified to include a similar requirement.<sup>74</sup> The ALRC had considered this but rejected it because of the operation of s 95B of the *Privacy Act 1988* (Cth), which already requires Commonwealth agencies to impose contractual obligations on third party contractors to comply with privacy principles.<sup>75</sup>

### The Commission’s view

2.46 In contrast to the ALRC, we consider that there is merit in clarifying whether the outsourcing agency or a contracted service

---

72. *Information Privacy Act 2000* (Vic) s 17. See, for example, *Complaint AG v Local Council* [2007] VPrivCmr 2 (8 June 2007); Office of the Victorian Privacy Commissioner, *Submission to the Australian Law Reform Commission’s Review of Australian Privacy Law (Discussion Paper No 72)* (2007) 20.

73. Inner City Legal Centre, *Submission*, 12; Public Interest Advocacy Centre, *Submission*, 16.

74. See NSWLRC Report 123, [8.76]. A “contracted service provider” for a government contract is defined to mean “(a) an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a State or Territory authority under the government contract; or (b) a subcontractor for the government contract”: *Privacy Act 1988* (Cth) s 6.

75. See NSWLRC Report 123, [8.30], [8.64]-[8.65].



provider is liable for an interference with privacy. This is because the difficult questions of principle attending the law of vicarious liability in relation to independent contractors,<sup>76</sup> combined with the doctrine of privity of contract, create uncertainty as to the rights of individuals to enforce the principles in the privacy regime.

2.47 The suggestion that the agency should remain responsible for the information while it is subject to dealings with a third party has much appeal. For the individual whose privacy has been infringed, it is much easier to identify the respondent to a privacy claim and provide more certainty in enforcement. On the other hand, it may strain an outsourcing agency's resources to provide continuing oversight of contractors' compliance and may unduly create litigation as the agency is left to pursue indemnity against the service provider.

2.48 A variant of the model in the Victorian and Queensland legislative schemes addresses these difficulties, whereby an agency entering into a contract with a contracted service provider continues to be liable for breaches of privacy principles unless it takes steps to ensure that the service provider is contractually required to comply with the relevant privacy principles. However, it may also create problems with enforcement for the individual whose privacy is breached.

2.49 We are of the view that expanding the definition of "public sector agency" to include a contracted service provider is not the solution to these problems. Contracted service providers are also likely to provide services that are not provided pursuant to a contract with a public sector agency. Where a contracted service provider does this, the classification of the provider, as a "public sector agency", is likely to create confusion as to whether this will mean that the provider is subject to other non-privacy related public sector agency obligations. Further, compliance with PPIPA by a contracted service provider can be achieved in other ways, such as through contractual provisions between the public sector agency and the service provider.

2.50 We remain of the view that UPP 8 should include a requirement to ensure the security of personal information disclosed to a third party in an outsourcing arrangement.<sup>77</sup> Further, as we recommended in Report

---

76. See *Sweeney v Boylan Nominees* (2006) 227 ALR 46.

77. See NSWLRC Report 123, Recommendation 10.

123,<sup>78</sup> a provision similar to s 95B of the *Privacy Act 1988* (Cth) should be adopted, requiring agencies to incorporate the privacy principles into contracts with third party contractors. If an agency engages the services of a contracted service provider, the agency should remain liable for any contraventions of privacy legislation.

## RECOMMENDATION 2.5

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to require an agency entering into a contract for the provision of services with a contracted service provider:

- (1) to take contractual measures to ensure that the contracted service provider does not perform an act, or engage in a practice, that would breach the privacy principles if performed or engaged in by the agency; and
- (2) to ensure that the contract does not authorise the contracted service provider to perform or engage in such an act or practice.

## MINISTERS

2.51 Finally, NSW ministers are not covered under either the *Privacy Act 1988* (Cth)<sup>79</sup> or PPIPA. However, the definition of “agency” in the GIPA Act expressly extends the NSW access to information regime to a Minister (including a Minister’s personal staff),<sup>80</sup> and the *Privacy Act 1988* (Cth) extends to federal Ministers. In the interests of uniformity, and in the absence of a compelling reason to the contrary, we are of the view that NSW Ministers should be subject to the requirements under PPIPA.<sup>81</sup>

78. NSWLRC Report 123, Recommendation 11.

79. “A State or Territory Minister” is excluded from the operation of the *Privacy Act 1988* (Cth): s 6C(3)(a).

80. *Government Information (Public Access) Act 2009* (NSW) s 4(1)(b).

81. See Office of the Privacy Commissioner, *Special Report to NSW Parliament under section 65 of the Privacy and Personal Information Protection Act 1998: Complaint by Student A and his father against Hon John Aquilina MP, Mr Walt Secord and Mr Patrick Low*, 7 May 2002. In that report, the Commissioner found that Mr Aquilina had played a role in violating the privacy of a student and his family and recommended that the student and his family receive an unqualified public apology from Mr Aquilina.

## RECOMMENDATION 2.6

The definition of "public sector agency" in the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include NSW Ministers.

## IDENTIFYING THE RELEVANT AGENCY

2.52 In the course of our inquiry, a question arose as to the potential difficulties involved in identifying clearly the relevant agency responsible for privacy management. Concerns were raised in the context of the conventional distinction in NSW government administration between the holder of a sole office and the staff supplied to the office to support the office-holder in the performance of her or his functions, for example, as between the NSW Ombudsman and the Office of the Ombudsman, the Director of Public Prosecutions and the Office of the Director of Public Prosecutions. Often the holder of the office is governed and established by a specific NSW enactment, with its own particular privileges and immunities,<sup>82</sup> whereas the support staff are generally covered by the *Public Sector Management Act 1988* (NSW).<sup>83</sup>

2.53 A second concern was raised in relation to identifying the agency at the proper level of responsibility, whether, for example, the correct respondent to a claim for interference with privacy is the particular agency within the relevant government department or the government department itself.

2.54 Our view is that neither of these issues need be addressed by legislation. The former issue was effectively dealt with in *CP v NSW Ombudsman*,<sup>84</sup> which was concerned with whether the Administrative Decisions Tribunal ("ADT") had jurisdiction to hear and decide an application for review of the NSW Ombudsman's Office in light of the immunity from civil proceedings granted to "the Ombudsman" and "an

82. See, for example, the *Ombudsman Act 1974* (NSW) s 35A, which confers an immunity on "the Ombudsman" and "an officer of the Ombudsman" in relation to "any civil, or criminal proceedings in respect of any act, matter or thing done or omitted to be done for the purpose of executing this or any other Act unless the act, matter or thing was done, or omitted to be done, in bad faith".

83. See *Public Sector Management Act 1988* (NSW) sch 1 which lists the "Departments" of government for the purposes of the Act, including the Ombudsman's Office, and the Office of the Director of Public Prosecutions.

84. *CP v NSW Ombudsman* [2002] NSWADT 103.

officer of the Ombudsman” under s 35A and s 35B of the *Ombudsman Act 1974* (NSW). The Ombudsman argued that he and or his officers did not constitute a “public sector agency” for the purposes of PPIPA and was thus not subject to review under the Act. The ADT rejected the argument that a distinction can be discerned in the scheme of PPIPA as between a public sector official and a public sector agency. It found that the “Ombudsman’s Office” was “simply another way of describing the group covered by the expression ‘officers of the Ombudsman’” and that the Office as a whole can be seen as a “public sector agency” for the purposes of the PPIPA. The Tribunal noted that:

the Ombudsman is the head of that Office, and his official conduct (even if later found to be outside his powers) can be treated as the conduct of the administrative Office; and similar [to] the conduct undertaken by staff in the Office under his authority (even if the conduct is later found to be outside power) can be treated as the conduct of the personal office of Ombudsman.<sup>85</sup>

Thus, it would seem that it would make no difference whether the holder of a sole office or the office itself was named as the respondent to privacy proceedings in the ADT.

2.55 The second concern may be dealt with in terms of the principles relating to accuracy in pleadings. As was noted in *Wood v The State of NSW*, this is always an issue that arises when actions are pleaded against the government:

It is important that the correct identity of the government agency or instrumentality be identified in the pleading and that the legislative basis for such identification be pleaded. Because although a party may have a right of action against an arm of government, it is not necessarily the case that the arm of government is simply, as is alleged in this case, the State of New South Wales.<sup>86</sup>

2.56 The correct identification of the relevant respondent and the question of whether the relevant agency is capable of suing or being sued in its own right, name and title, or whether the Crown is the appropriate respondent, may be determined from an examination of the legislative framework around which the entity was established.<sup>87</sup>

---

85. *CP v NSW Ombudsman* [2002] NSWADT 103, [20].

86. *Wood v The State of NSW* [2008] FMCA 566, [18].

87. *Wood v The State of NSW* [2008] FMCA 566, [17].





## 3. **Consent**

- Introduction
- Consent in NSW privacy law
- Third party agents
- Young people

## INTRODUCTION

3.1 This chapter examines three major issues in relation to consent:

- the nature and role of consent in privacy law;
- what happens where people lack capacity to consent and require a third party to act for them; and
- whether there should be special rules dealing with incapacity to consent where that incapacity arises because the individual is under the age of majority.

3.2 The recommendations in this chapter will propose action for the Office of the Privacy Commissioner (“Privacy NSW”). Whether Privacy NSW will be the appropriate body to carry out the proposed actions will depend upon the NSW Government’s response to our recommendations in Report 125.<sup>1</sup>

## CONSENT IN NSW PRIVACY LAW

### What relevance is consent to privacy law?

3.3 In Report 120, we recommended that a plaintiff could not succeed in a statutory action for invasion of privacy if he or she had consented to the defendant’s conduct.<sup>2</sup> In the context of the statutory regulation of information privacy, the Australian Law Reform Commission (“ALRC”) recommended that consent should not be an independent privacy principle lest it become the overriding factor in allowing or restricting the handling of personal information.<sup>3</sup> Consent therefore features in the proposed Unified Privacy Principles (“UPPs”) as an exception to a general privacy principle or as a basis to authorise the handling of particular information in a certain way. It is particularly relevant to the

- 
1. We recommend that the Office of the Information Commissioner (“OIC”) should be the sole statutory authority responsible for the administration of privacy and freedom of information in NSW. We recommend that the OIC should contain a Privacy Division responsible for administration and oversight of privacy legislation: See NSW Law Reform Commission, *The Offices of the Information and Privacy Commissioners*, Report 125 (2009).
  2. NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) [5.46]-[5.53].
  3. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”) vol 1, [19.69]-[19.77].



principles concerning the collection of sensitive information and use and disclosure. In Report 123, we generally endorsed the UPPs.<sup>4</sup>

## The current framework

### *PPIPA*

3.4 The *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”) does not define “consent” and it is unclear whether consent must be express or implied, either generally or in relation to specific provisions.<sup>5</sup> Consent is relevant to a number of the Information Protection Principles (“IPPs”) contained in PPIPA. A variant of the word “consent” is first used in s 9 of PPIPA, which provides that a public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless the individual has authorised collection of the information from someone else, or the individual is aged under 16 years and a parent or guardian of the individual has authorised collection of the information.

3.5 A variant of consent is also relevant to s 18, although the word is neither expressly nor impliedly used. Section 18 sets out that a public sector agency must not disclose personal information to a person or other body unless one of three circumstances exist including that the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure.

3.6 The word “consent” is expressly used in s 17, which stipulates that information can only be used for the limited purpose for which it was collected unless the individual to whom the information relates has consented to the use of the information for another purpose. Consent, however, is not required under s 17 where the use of the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another person.

3.7 The word “consent” is also used in s 19, which provides that sensitive information can only be disclosed with consent, or without consent to deal with a serious and imminent threat to any person’s health or safety.

---

4. See NSW Law Reform Commission, *Privacy Principles*, Report 123 (2009).

5. But see *Privacy and Personal Information Protection Act 1998* (NSW) s 26(2).

3.8 “Consent” is also relevant to s 26(2) of PPIPA, which provides that a public sector agency is not required to comply with s 10, s 18 or s 19 of PPIPA<sup>6</sup> if the individual to whom the information relates has expressly consented to the agency not complying with the principle concerned.<sup>7</sup>

#### *HRIPA*

3.9 The *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”) does not define “consent”. Section 7, however, deals with the capacity of an individual to do an act authorised, permitted or required by the Act. Section 7(1) provides that:

An individual is incapable of doing an act authorised, permitted or required by [HRIPA] if the individual is incapable (despite the provision of reasonable assistance by another person) by reason of age, injury, illness, physical or mental impairment of:

- (a) understanding the general nature and effect of the act, or
- (b) communicating the individual’s intentions with respect to the act.

3.10 “Consent” is relevant to the Health Privacy Principles (“HPPs”) contained in HRIPA. HPP 4 provides that an organisation (which includes a public sector agency)<sup>8</sup> that collects health information about an individual from the individual must ensure that the individual is aware of certain matters including the identity of the organisation, how to contact the organisation and the purposes for which the information is collected. HPP 4 also provides that an organisation is not required to make an individual aware of the matters provided in HPP 4 if the individual to whom the information relates has expressly consented to the organisation dispensing with that requirement.<sup>9</sup>

---

6. *Privacy and Personal Information Protection Act 1998* (NSW) s 10, s 18 and s 19 deal with the requirements of an agency when collecting personal information, the limits on disclosure of personal information and the special restrictions on disclosure of personal information.

7. See para 6.24-6.26.

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

9. Importantly, fulfilling these notification obligations does not amount to seeking consent and must not be confused with consent: see NSW Law Reform Commission, *Privacy Legislation in New South Wales*, Consultation Paper 3 (2008) (“NSWLRC CP 3”) [3.78].

3.11 The word “consent” is also used in HPP 10, which sets out a number of exceptions to the general requirement that an organisation holding health information should not use the information for a purpose (a “secondary purpose”) other than the purpose for which it was collected. One such exception is that the individual to whom the information relates has consented to the use of the information for that secondary purpose. Similarly, HPP 11 provides that an organisation that holds health information must not disclose the information for a secondary purpose unless the individual to whom the information relates has consented to the disclosure.

3.12 “Consent” is also relevant to HPP 12 which sets out that a “private sector person” may only adopt an identifier of an individual that has been assigned by a public sector agency in limited circumstances, one of which is that the individual has consented to the adoption of the same identifier. Similarly, under HPP 14, an organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside NSW or to a Commonwealth agency unless the individual consents to the transfer.

3.13 The word “consent” also appears in HPP 15, which provides, subject to certain exceptions, that 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.

3.14 HPPs 10, 11 and 12 differ from HPPs 4, 14 and 15 insofar as they do not indicate that the consent needs to be express. It is not clear, however, whether consent can be implied for the purposes of HPPs 4, 14 and 15.

#### *Privacy codes*

3.15 The issue of consent is also relevant to the operation of a number of codes made pursuant to PPIPA and HRIPA. For example, cl 10(2) of the *Privacy Code of Practice (General) 2003* (NSW) (“General Code”), provides that despite the IPPs, a human services agency may collect and use personal information about an individual, and may disclose personal information about the individual to another human services agency or allied agency, if the collection, use or disclosure is in accordance with a written authorisation given by a senior officer of the agency. Sub-clause 10(4) sets out that a senior officer may give an authorisation under cl 10(2) only if the officer is satisfied of a number of circumstances, including that the individual (or a person authorised by or under PPIPA or any other law to give consent on the individual’s behalf) has failed to consent to the

agency collecting or using the specified information or disclosing the specified information to the specified agencies. A similar regulation exists in the *Health Records and Information Privacy Code of Practice 2005* (NSW).<sup>10</sup>

## The elements of consent

3.16 Consent in privacy law can mean several things:<sup>11</sup>

- it can refer to an individual’s capacity;
- it can refer to the necessity of legally relevant conduct being voluntary;
- it can refer to the sufficiency of a knowledge base on which a person’s decision to act, or not act, was taken;
- it can refer to the need for consent to be specific; or
- it can refer to the necessity for consent to be current.

### *Capacity*

3.17 An individual is regarded as having capacity if he or she is able to understand the general nature and effect of a particular decision or action and is able to communicate his or her consent, or refusal of consent, to the decision or action.<sup>12</sup> Generally speaking, the law presumes that individuals have the capacity to consent, although there are exceptions to this presumption for some individuals such as those who are mentally ill or very young.

3.18 In Report 119 we made the following observations about the concept of capacity:

Capacity sets a minimum standard of decision-making skills that is required in order to recognise the validity of a person’s decision. If these skills are diminished in a particular individual because of some impairment and do not reach this minimum standard, then the law will not allow that person’s decision to be acted upon because it cannot be said to reflect a real choice made by a free-thinking individual.<sup>13</sup>

---

10. See *Health Records and Information Privacy Code of Practice 2005* (NSW) cl 4.

11. Privacy NSW Best Practice Guide: *Privacy and People with Decision-making Disabilities* (2004) [3.1] (“Privacy NSW Best Practice Guide”). See NSW Law Reform Commission, *Young People and Consent to Health Care*, Report 119 (2008) (“NSWLRC Report 119”) [1.5]-[1.6].

12. Privacy NSW Best Practice Guide, [3.2].

13. NSWLRC Report 119, [1.7].

3.19 Privacy NSW notes that there are a number of characteristics to capacity, including that capacity is unique to the individual; is not static; depends on the nature of the decision to be made; and depends on the support to be provided to make the decision. Privacy NSW also stresses that assumptions about a person’s cultural and linguistic background should not influence judgments about capacity and that a person does not need to make what other people might regard as a “good” or “right” decision, or a decision that may be in the person’s best interests, in order for that person to be considered to have capacity.<sup>14</sup>

#### *Voluntariness*

3.20 Consent will generally be considered to have been given voluntarily where the individual giving it had a clear option or opportunity not to consent.<sup>15</sup> In determining whether consent has been given voluntarily, it is often necessary to consider whether the option not to consent involved no financial cost to, and little effort from, the individual. It may sometimes be difficult to determine whether a person has voluntarily given consent as coercion may be implicit. For example, a threat to withdraw or not provide services if consent is not given might amount to implicit coercion to consent.<sup>16</sup>

#### *Informed consent*

3.21 A number of existing guidelines, international instruments, regional models, and overseas legislation relating to privacy consider that consent must be informed for it to be valid.<sup>17</sup> While the concept of “informed consent” is often difficult to separate from capacity,<sup>18</sup> the focus of informed consent is that an individual must have reasonable knowledge of all relevant facts before he or she gives or refuses consent.<sup>19</sup> An individual must be aware of the implications of providing or

---

14. Privacy NSW Best Practice Guide, [3.3].

15. See Australia, Office of the Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001) [A.5.2]; European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), art 2(h); G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0*, 3 September 2003 (2003) WorldLII Privacy Law Resources, <[www.worldlii.org/int/other/PrivLRes/2003/1.html](http://www.worldlii.org/int/other/PrivLRes/2003/1.html)> at 12 February 2010, Principle 2.

16. Privacy NSW Best Practice Guide, [3.3].

17. See ALRC Report 108, vol 1, Chapter 19.

18. NSWLRC Report 119, [1.11]-[1.12].

19. Privacy NSW Best Practice Guide, [3.3].

withholding consent and must have received the relevant facts in a way meaningful to him or her and in a way that is appropriate in the circumstances.<sup>20</sup> Relevant facts might include, for example, the purpose or purposes of collecting the information and who will have access to what parts of the information.

### *Specific consent*

3.22 Consent must also be reasonably specific to meet the circumstances of each case.<sup>21</sup> The specificity required depends on a number of factors including the nature of the personal information and the proposed use or disclosure of the personal information, including future uses or disclosures. For example, consent to collect and use personal information to provide a particular financial product might not extend to consent to disclose that information to agencies offering complementary financial products. As a general rule, Privacy NSW suggests that the more privacy-intrusive the proposed use or disclosure, the more specific the notification and consent will need to be.<sup>22</sup>

### *Consent must be current*

3.23 It has also been suggested that consent must be current for it to be valid.<sup>23</sup> Privacy NSW notes that it cannot be assumed that consent given in particular circumstances will endure indefinitely with the passage of time and changes of circumstances. This consideration is particularly important where the person giving consent has a decision-making disability, the nature of which causes him or her to lose awareness of matters about which he or she was previously informed.

---

20. See Office of the Australian Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), [A.5.2]; European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995) art 2(h); G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0*, 3 September 2003 (2003) WorldLII Privacy Law Resources, <[www.worldlii.org/int/other/PrivLRes/2003/1.html](http://www.worldlii.org/int/other/PrivLRes/2003/1.html)> at 10 February 2010, Principle 2.

21. Privacy NSW Best Practice Guide [3.3]; European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995) art 2(h).

22. Privacy NSW Best Practice Guide, [3.3].

23. Privacy NSW Best Practice Guide, [3.3].

## The approach of the ALRC

3.24 The ALRC made three proposals in Discussion Paper 72 that aimed to clarify the meaning of consent as it applies to the privacy principles.<sup>24</sup> The first was to amend the *Privacy Act 1988* (Cth) so that it would detail the requirements for obtaining consent in the many contexts in which it may be sought and so that it would set out the factors that should be taken into account in obtaining an individual's consent. The second was that the Office of the Commonwealth Privacy Commissioner provide more guidance on what amounts to consent for the purposes of the privacy principles. The ALRC suggested that this guidance should cover consent as it applies in various contexts, and should include advice on when it is and is not appropriate to use bundled consent. The third proposal combined the first and second proposals.<sup>25</sup>

3.25 The second proposal gained greater support than the first and third proposals in submissions from stakeholders.<sup>26</sup> For example, stakeholders noted that guidelines would serve to clarify legislation, enhance compliance, promote consistent implementation, increase public awareness and maintain flexibility.<sup>27</sup> Stakeholders noted that this was preferable to amending the *Privacy Act 1988* (Cth) given the complexity of the issues surrounding consent<sup>28</sup> and the risk of increasing the complexity of privacy regulation without it being apparent that there was a deficiency in the current consent framework.<sup>29</sup> However, stakeholders also recognised the limitations of guidelines, including that, by definition, guidelines are generally not legally enforceable.<sup>30</sup>

3.26 A smaller number of stakeholders supported the third proposal on the grounds that further guidance from the Office of the Commonwealth Privacy Commissioner would not be sufficient and that the *Privacy Act 1988* (Cth) should be amended to include a more detailed definition of consent. It was suggested, for example, that the definition of consent

---

24. Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007) ("ALRC Discussion Paper 72").

25. ALRC Discussion Paper 72, [16.26]-[16.35]

26. ALRC Report 108, vol 1, [19.29]-[19.41].

27. ALRC Report 108, vol 1, [19.33].

28. ALRC Report 108, vol 1, [19.31].

29. ALRC Report 108, vol 1, [19.32].

30. ALRC Report 108, vol 1, [19.33].

include a non-exhaustive list of factors to be taken into account in determining whether a person's consent has been obtained.<sup>31</sup>

3.27 The ALRC was of the view that it was undesirable to amend the *Privacy Act 1988* (Cth) to provide what would be required to obtain valid consent in the various contexts in which it may be sought. It considered that this approach would involve the enactment of a significant number of prescriptive rules, which would not be in keeping with the ALRC's support for the retention of the principles-based approach of the *Privacy Act 1988* (Cth). It also noted the difficulty in drafting rules to cover every possible context in which consent may be relevant and the possibility that a statutory definition of consent would be interpreted very narrowly, leading to an undesirable restriction on the flow of information.<sup>32</sup>

3.28 Ultimately, the ALRC recommended that the Office of the Commonwealth Privacy Commissioner develop and publish further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act 1988* (Cth). It recommended that guidelines address the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained and cover express and implied consent as it applies in various contexts.<sup>33</sup>

3.29 The Commonwealth Government has accepted this proposal. It stated that it encourages the development and publication of appropriate guidance by the Office of the Commonwealth Privacy Commissioner and that it acknowledges that the decision to provide guidance is a matter for the Privacy Commissioner. The Commonwealth Government also indicated that it will expand the definition of "consent" to clarify that an individual may withdraw consent where it is lawful to do so. It foreshadowed that individuals will be able to withdraw consent in ways that accord with the principles of common or contractual law, but did not expand upon this proposal.<sup>34</sup>

---

31. ALRC Report 108, vol 1, [19.39].

32. ALRC Report 108, vol 1, [19.62].

33. ALRC Report 108, Recommendation 19-1.

34. Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice* (2009) 38.



## The Commission's view

3.30 Guidelines would go some way to ensuring that agencies and organisations do not mistakenly infer that consent has been given or has been withdrawn. This would enable individuals to exercise control over the collection, use and disclosure of their personal information. We have decided against recommending that the guidelines define “consent” given the complexity of the concept, preferring instead the current approach of Privacy NSW of considering the elements of consent. We support the approach of the Commonwealth Government and the ALRC.

### RECOMMENDATION 3.1

The Privacy Commissioner should consult with the Commonwealth Privacy Commissioner to produce guidelines for NSW agencies about what is required of agencies to obtain an individual's consent for the purposes of NSW privacy law. The guidelines should:

- (1) address the factors that agencies should take into account in assessing whether consent has been obtained; and
- (2) provide how consent can be withdrawn.

## Bundled consent

3.31 Bundled consent refers to the “bundling” together of more than one request for an individual's consent to a wide range of uses and disclosures of personal information, without providing the individual with the option of selecting the uses and disclosures to which he or she agrees.<sup>35</sup>

3.32 “Bundled consent” has attracted criticism on the grounds that it may mean that consent will not necessarily be given in a way that is meaningful, voluntary and informed.<sup>36</sup> It has also been suggested that agencies may abuse the practice by bundling together unrelated uses and disclosures of information and not providing consumers with the opportunity to consent to some uses and disclosures but not others.<sup>37</sup> However, some agencies (such as agencies in the business sector and the telecommunications sector) regard bundled consent as necessary to

35. Australia, Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005) 82.

36. ALRC Report 108, vol 1, [19.26].

37. ALRC Report 108, vol 1, [19.67].

achieve business efficiency and reduce costs to the consumer.<sup>38</sup> It might also be added that agencies may cause a consumer annoyance if they are constantly contacting him or her asking for his or her consent.<sup>39</sup>

3.33 In light of the benefits and detriments of using bundled consent, the ALRC saw a need to clarify the parameters of the practice of bundled consent, and the circumstances in which it is appropriate to rely on such consent. It recommended that this clarification occur through the development of guidelines, which would address the practice of bundled consent in specific industry sectors, such as finance, debt collection, credit reporting, telecommunications, and residential tenancy. It further recommended that the Office of the Commonwealth Privacy Commissioner develop guidance on bundled consent, in consultation with relevant stakeholders and industry sectors. We support this process for developing guidelines, as this is likely to ensure the relevance and practicality of such guidelines for each industry.

### RECOMMENDATION 3.2

The Privacy Commissioner should liaise with the Commonwealth Privacy Commissioner to produce guidelines for NSW agencies that include advice on when it is and is not appropriate to use “bundled consent”. The advice should be specific to industry sectors and should be formulated in consultation with relevant stakeholders, industry sectors and individuals.

### Express and implied consent

3.34 Consent can be express or implied. Express consent is consent that is clearly and unmistakably communicated and may be provided in writing, orally or in any other form. Implied consent is consent that can reasonably be inferred from an individual’s conduct or actions. Privacy NSW has expressed concern with allowing agencies to rely on implied consent noting that it can be difficult to determine whether an individual has genuinely consented without the individual expressing consent.<sup>40</sup>

3.35 Several submissions stated that the law is currently unclear as to what amounts to express consent and what amounts to implied consent

38. ALRC Report 108, vol 1, [19.27].

39. ALRC Report 108, vol 1, [19.51].

40. Privacy NSW Best Practice Guide, [3.4].

and when one or the other is required.<sup>41</sup> For example, the HIV/AIDS Legal Centre expressed concern about the lack of clarity as to whether consent must be express or implied for the purposes of HRIPA. It proposed that the definition of consent be clarified and that legislation make clear when consent needs to be express and when it can be implied. The HIV/AIDS Legal Centre was particularly concerned about the transfer of HIV-related information and proposed that express consent be required for the transfer of such information.<sup>42</sup>

3.36 The Statutory Review of PPIPA recommended that PPIPA provide for implied consent to agencies handling a person's personal information in appropriate circumstances.<sup>43</sup> This recommendation was made in response to a submission from the Department of Housing that an express statutory recognition of implied consent, would, in certain circumstances, assist in responding to the concerns of clients. The Statutory Review of PPIPA did not, however, indicate whether the Department of Housing elaborated upon this submission or provided an example. The recommendation was also made in light of the *Privacy Act 1988* (Cth) and the *Information Privacy Act 2000* (Vic), which both define consent to include express and implied consent.<sup>44</sup> In its response to the Statutory Review of PPIPA, the NSW Government stated that while it supported this recommendation in principle, it would consider the issue further after the reports of the ALRC and NSWLRC had been tabled.<sup>45</sup> In its report, the ALRC recommended that the Office of the Commonwealth Privacy Commissioner produce guidelines that cover express and implied consent as it applies in various contexts.<sup>46</sup> We support this approach.

---

41. The HIV/AIDS Legal Centre, *Submission*, 13; Sydney Opera House, *Preliminary Submission*, 1.

42. The HIV/AIDS Legal Centre, *Submission*, 13.

43. NSW Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly) ("Statutory Review of PPIPA") Recommendation 10.

44. Statutory Review of PPIPA, [7.9]-[7.10].

45. NSW Government, *Response to the Report on the Statutory Review of the Privacy and Personal Information Protection Act 1998*, 6. *Privacy Act 1988* (Cth) s 6 and *Information Privacy Act 2000* (Vic) s 3 both provide that "consent" means express consent or implied consent.

46. ALRC Report 108, Recommendation 19-1.

**RECOMMENDATION 3.3**

The Privacy Commissioner should liaise with the Commonwealth Privacy Commissioner to produce guidelines for NSW agencies that cover express and implied consent as it applies in various contexts.

**THIRD PARTY AGENTS**

3.37 An individual may not have the requisite capacity to consent by reason of age, injury, illness, or physical or mental impairment, and may therefore require that a third party act on his or her behalf or provide assistance. Some individuals may require the assistance of a third party because of language barriers or other communicative barriers but still have the capacity to provide the requisite consent. Such individuals may seek assistance from a carer, a parent, a spouse, an adult child, a close friend, an interpreter, a relative, a counsellor or a legal representative and may do so on a temporary or permanent basis or pursuant to a one-off or short-term arrangement.

**Current framework***PPIPA and HRIPA*

3.38 PPIPA is generally silent as to how an individual who has a decision-making disability is to provide any requisite consent sought by the Act.<sup>47</sup>

3.39 Section 7 of HRIPA provides that an individual who is incapable of doing an act authorised, permitted or required by the Act may have an “authorised representative” who may act on the individual’s behalf. It further provides that an “authorised representative” may not act on behalf of an individual who is capable of doing that act, unless the individual expressly authorises the authorised representative to act. “Authorised representative” is defined in s 8 of HRIPA to mean an attorney acting under an enduring power of attorney; a guardian within the meaning of the *Guardianship Act 1987* (NSW); a person responsible within the meaning of Part 5 of the *Guardianship Act 1987* (NSW); or a person having parental responsibility for the individual, if the individual

---

47. Although note *Privacy and Personal Information Protection Act 1998* (NSW) s 9(a) (IPP 2) which provides that a public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless the individual has authorised collection of the information from someone else.

is a child; or a person who is otherwise empowered under law to exercise any functions as an agent of, or in the best interests of, the individual.

3.40 The Statutory Review of PPIPA noted that some service delivery agencies had expressed concern that there is no substitute consent regime in an Act that is so heavily reliant on consent.<sup>48</sup>

*Privacy codes and directives*

3.41 Schedule 3 to the *General Code*, modifies the IPPs that apply to ageing disability and home care service agencies (“ADHCs”) to the extent that in many instances, an ADHC need not strictly comply with an IPP where the individual to whom personal information relates lacks the capacity to provide the requisite consent or authority. Instead, an ADHC can obtain consent from the “personal information custodian” of an individual lacking capacity, which is defined in cl 17 of the *General Code* to include the individual’s guardian; attorney; spouse, if the relationship between the individual and the spouse is close and continuing; carer; or close friend or relative.

3.42 The NSW Department of Ageing, Disability and Home Care (“DADHC”) submitted that the operation of the *General Code* overcomes the difficulties that DADHC might otherwise face if it was required to comply with s 9 of PPIPA (which requires an agency to collect personal information directly from the individual). DADHC submitted that it would not be possible to comply with this principle because many of the people from whom it collects information have a decision-making disability. DADHC suggested that the principles enunciated in the *General Code* be incorporated in PPIPA itself.<sup>49</sup>

3.43 Another existing arrangement is that outlined in the “Direction for the Department of Human Services and Associated Agencies”,<sup>50</sup> which modifies the IPPs as they apply to the Department of Human Services and associated agencies. Pursuant to the direction, consent must be sought from the next most appropriate person in matters involving collection, use and disclosure of personal information pursuant to PPIPA where an individual is unable to provide fully informed consent to the collection, use or disclosure of personal information relating to him or

---

48. Statutory Review of PPIPA, [7.3].

49. NSW Department of Ageing, Disability and Home Care, *Submission*, 2.

50. NSW Privacy Commissioner, “Direction for the Department of Human Services and Associated Agencies”, Public Interest Direction (23 December 2009).

her; is 16 years of age or over; and does not have a legally appointed guardian with power to make a decision on his or her behalf regarding the information. Such consent can only operate where reasonable steps have been taken to involve the individual in the consent process. “Most appropriate person” is defined in cl 1 of the Direction to include any individual coming under the definition of persons responsible as defined in s 33A of the *Guardianship Act 1987* (NSW) or an advocate appointed to represent a particular individual’s best interests.

#### *Privacy NSW guidelines*

3.44 In response to the gaps in NSW legislation, Privacy NSW published a *Best Practice Guide* in February 2004 to assist agencies which deal with people with decision-making disabilities.

3.45 Privacy NSW identifies two main alternative decision-making models namely one where a decision is made on behalf of the individual by a representative (substitute model) and one where a decision is made on behalf of the individual by an agency or organisation using objective criteria (procedural model).

3.46 ***Substitute model.*** Under the substitute model, a person “stands in the shoes” of the person with a decision-making disability and makes the decision on his or her behalf. While some individuals with a decision-making disability have a guardian or a manager appointed by law to manage particular areas of his or her life, such as his or her living and personal care arrangements or his or her medical and dental treatment, many people with a decision-making disability do not have a legally appointed guardian. Importantly, even if an individual has such a legal arrangement, the legal arrangement may not pertain to all of the individual’s personal affairs and may not include decisions relating to the collection and use and disclosure of the individual’s personal information.

3.47 Privacy NSW provides a list of who a person’s representative may be, which includes an attorney for the individual under an enduring power of attorney; a guardian within the meaning of the *Guardianship Act 1987* (NSW); a person responsible within the meaning of the *Guardianship Act 1987* (NSW); and a person who is otherwise empowered under law to exercise any functions as an agent of, or in the best interests of, the person in relation to decisions about personal information that are consistent with the scope of the legal authority.

3.48 The list is by no means exhaustive and Privacy NSW recommends that agencies apply a flexible definition of a person's representative. It stresses that the appropriateness of the representative may depend upon the type of information that the agency is concerned with. It provides the example of a financial manager appointed under a court or tribunal order who should be able to represent the person in relation to decisions about his or her financial information to the extent authorised by his or her appointment, but who may not be appropriate to represent the person in relation to other types of personal information such as information about lifestyle decisions.

3.49 Privacy NSW recognises that in some circumstances, it may not always be possible to use the substitute model, such as where an individual does not have someone who can act on his or her behalf or where the individual's interests conflict with the views of his or her substitute decision-maker or where family members cannot agree upon the best interests of their relative.<sup>51</sup>

3.50 *Procedural model.* Under the procedural model, clear and consistent criteria are used to determine whether the information handling practice proposed by the agency is in the best interests of the individual. Privacy NSW recommends that the agency set out in writing what criteria will be applied to make a final decision about what will happen to the individual's information. It suggests that the criteria the agency might use include matters such as the type of personal information being collected; who will collect the information; the purpose of collection; the intended recipients of the information; whether the person and/or his or her representative has been notified of the relevant matters in a manner that is appropriate to his or her capacities and linguistic and cultural background and any views expressed by the person about how his or her information may be used.

3.51 Privacy NSW recommends that agencies applying the procedural model document all the relevant criteria and the final decision about what happens to a person's information, particularly in cases where the proposed information handling practice is privacy-intrusive.

3.52 In light of the strengths and weaknesses of both models, Privacy NSW ultimately proposes that agencies use a combination of substitute and procedural decision-making procedures where it is not possible for

---

51. Privacy NSW Best Practice Guide, [4.3].

the agency to comply strictly with the requirements of PPIPA because of an individual's decision-making disability. Such a flexible and integrated approach is considered more likely to fit the unique circumstances of each individual and promote the accountability of an agency when it handles personal information about the individual.

3.53 Importantly, Privacy NSW emphasises that even if an individual's decisions are made by another person, the individual should be involved as much as possible in the decision-making process. It recommends that agencies take reasonable steps to provide information and support that is sensitive to the capacities of the individual as well as his or her cultural and linguistic background so that he or she can participate meaningfully in the decision-making. For example, an agency might adopt a pictorial format to explain issues to people who have an intellectual disability. Privacy NSW also suggests that if an agency is aware that an individual with a decision-making disability made his or her wishes about his or her personal information known to others at a time when he or she had capacity (or could become aware of such previous wishes by taking reasonable steps), it should consider his or her previously expressed wishes with other relevant criteria when handling the information.<sup>52</sup>

### Submissions and consultations

3.54 A number of stakeholders recognised the need for a scheme of substitute decision-making to enable decisions to be made for people who have a decision-making disability. These stakeholders were of the view that PPIPA should be amended to introduce a provision equivalent to s 7 of HRIPA (which provides a test as to when an individual is considered incapable of doing an act required under HRIPA).<sup>53</sup> There was also a suggestion that PPIPA contain provisions similar to those in relevant Victorian legislation,<sup>54</sup> which allows an authorised representative to provide consent on behalf of an individual incapable of giving consent if

---

52. Privacy NSW Best Practice Guide, [4.3].

53. Cyberspace Law and Policy Centre, *Submission*, 20; Inner City Legal Centre, *Submission*, 35; NSW Health, *Submission*, 6; Business Law Committee of the Law Society of NSW, *Submission*, 10; NSW FOI/Privacy Practitioners Network, *Submission*, 7; NSW Guardianship Tribunal, *Submission*, 1.

54. NSW Health, *Submission*, 6.



the consent is “reasonably necessary for the lawful performance of functions or duties or exercise of powers in respect of the individual”.<sup>55</sup>

3.55 The Intellectual Disability Rights Service (“IDRS”) was of the view that where an agency collects the personal information of a person with an intellectual disability, the agency should explain the personal information collection and use in a way the person will be able to understand. For example, explanations could be drafted in plain English or could use pictures and might take a written or oral form. The IDRS suggested that the onus should be on the agency to ensure that an individual with an intellectual disability can understand how his or her personal information will be collected and used. It also advocated that an individual’s capacity be assessed on a case-by-case basis to reflect the fact that the capacity of a person with an intellectual disability may change depending on the complexity of the decision to be made. The IDRS was of the view that the substitute decision maker should at least include a guardian or “person responsible” as defined in the *Guardianship Act 1987* (NSW).<sup>56</sup>

3.56 A number of stakeholders commented favourably on Privacy NSW’s *Best Practice Guide*. As already noted, DADHC suggested that the document be examined with a view to identifying what aspects of it could be incorporated as amendments to PPIPA and/or HRIPA.<sup>57</sup> The Office of the Protective Commissioner has similarly expressed approval for the *Best Practice Guide* and has recommended that mental health professionals implement the recommendations in the *Best Practice Guide*.<sup>58</sup>

---

55. *Information Privacy Act 2000* (Vic) s 64(1) and s 64(2)(b). Under s 64(3), the test for determining whether an individual is incapable of providing consent is whether “he or she is incapable by reason of age, injury, disease, senility, illness, disability, physical impairment or mental disorder of (a) understanding the general nature and effect of giving the consent” or “(b) communicating the consent or refusal of consent” despite “the provision of reasonable assistance by another individual”.

56. The IDRS was of the view that this practice may also assist others in the community who have reduced capacity to understand the personal information collection and use process, such as elderly people, people from culturally and linguistically diverse backgrounds, people with literacy problems, people with learning disabilities, people with a vision-impairment, people with acquired brain injury, people with a developmental disability and people living with dementia: Intellectual Disability Rights Service, *Submission*, 3-5.

57. NSW Department of Ageing, Disability and Home Care, *Submission*, 2.

58. NSW Office of the Protective Commissioner, *Preliminary Submission*, 3.

Furthermore, the list in the *Best Practice Guide* as to who can be a person's representative incorporates the suggestion of the NSW Guardianship Tribunal that an "authorised representative" include those who fall within the "person responsible" scheme under the *Guardianship Act 1987* (NSW).<sup>59</sup>

3.57 The Guardianship Tribunal, however, contended that an "authorised representative" may only be helpful to an individual who either had capacity at some stage and so was able to choose his or her substitute decision maker or who is involved in the guardianship system and has had a guardian formally appointed.<sup>60</sup>

3.58 The submissions also identified areas in need of clarification. There was support for clear legislative provisions that allow people supporting individuals with a decision-making disability to access information to enable them to undertake their role. The Office of the Protective Commissioner stressed that such information be limited to that which is "absolutely necessary" to enable the person assisting to care for the individual appropriately.<sup>61</sup> Similarly, the Guardianship Tribunal argued that there was a need to amend privacy laws to allow agencies to provide the Guardianship Tribunal with personal and health information about people with decision-making disabilities who are unable to provide the requisite consent for the release of that information and who do not have a substitute decision maker to provide that consent.<sup>62</sup> Further, the Office of the Protective Commissioner submitted that there is some debate as to whether a financial management order also confers powers to make privacy decisions. For example, the Protective Commissioner may be appointed to make decisions as if he or she was the person the subject of the financial management order, but it is not clear whether this order allows the Protective Commissioner to act as a substitute decision maker and provide consent in relation to the collection, storage and handling of that person's personal and sensitive information.<sup>63</sup>

3.59 The NSW Government has already expressed its support for allowing third parties to provide information to agencies, where

---

59. NSW Guardianship Tribunal, *Submission*, 4.

60. NSW Guardianship Tribunal, *Submission*, 3.

61. NSW Office of the Protective Commissioner, *Preliminary Submission*, 3.

62. NSW Guardianship Tribunal, *Submission*, 1.

63. NSW Office of the Protective Commissioner, *Preliminary Submission*, 1.

appropriate. In its response to the Statutory Review of PPIPA, the NSW Government supported the recommendation in the report that s 9 of PPIPA be amended so that collection from a third party is permitted where it is unreasonable or impracticable to collect the information from the individual to whom the information relates.<sup>64</sup> The Government noted that the absence in PPIPA of a provision permitting collection of personal information from third parties where an individual cannot provide the requisite consent causes most agencies some difficulty in their day-to-day operations. The Government expressed the view that amending s 9 of PPIPA, if supported by the NSWLRC and the ALRC, may alleviate these problems.<sup>65</sup>

### The approach of the ALRC

3.60 Like PPIPA, the *Privacy Act 1988* (Cth) is silent as to possibility of third parties acting on behalf of individuals. The ALRC recommended that the Office of the Commonwealth Privacy Commissioner develop and publish guidance that would assist agencies and organisations to understand how relevant guardianship and administration and power of attorney legislation applies in the context of the *Privacy Act 1988* (Cth).<sup>66</sup> This recommendation was made in response to concerns raised in submissions that some agencies and organisations do not give appropriate recognition to substitute decision makers authorised by law. The ALRC was of the view that this problem was the result of a lack of understanding by agencies and organisations of the guardianship and administration and power of attorney laws that apply in each State and Territory.<sup>67</sup>

3.61 The ALRC also recommended amending the *Privacy Act 1988* (Cth) to provide greater certainty to arrangements that allow an individual to nominate a third party to act on his or her behalf. In particular, the ALRC suggested that the *Privacy Act 1988* (Cth) be amended to include the concept of a “nominee” and provide that an agency or organisation may establish nominee arrangements. The agency or organisation could then

---

64. The NSW Government chose, however, to defer further consideration of this recommendation until the reports of the NSWLRC and the ALRC on privacy law had been tabled.

65. See NSW Government, *Response to the Report on the Statutory Review of the Privacy and Personal Information Protection Act 1998*, 4.

66. ALRC Report 108, vol 3, [70.5].

67. ALRC Report 108, vol 3, [70.61].

deal with the nominee as if he or she were the individual.<sup>68</sup> The ALRC anticipated that the nominee arrangement would provide an effective remedy for an individual and his or her informal representatives where incapacity is anticipated, such as where the individual is in the early stages of dementia, and the nomination is made prior to the loss of capacity.<sup>69</sup> The nominee arrangement was also seen as a flexible approach that recognised that an individual's capacity can change over time.<sup>70</sup>

3.62 The ALRC recommended that key elements of the nominee arrangement be incorporated into the *Privacy Act 1988* (Cth) and that such arrangements provide sufficient flexibility for an agency or organisation to be able to develop administrative arrangements appropriate to the context in which it operates.<sup>71</sup> It contended that a legislative provision would ensure that the nomination would have an enduring quality and would help raise awareness of such arrangements.<sup>72</sup>

3.63 The ALRC was of the view that *Privacy Act 1988* (Cth) should include, at a minimum, that:

- (a) a nomination can be made by an individual or a substitute decision maker authorised by a federal, state or territory law;
- (b) the nominee can be an individual or an entity;
- (c) the nominee has a duty to act at all times in the best interests of the individual; and
- (d) the nomination can be revoked by the individual, the nominee or the agency or organisation.<sup>73</sup>

3.64 The ALRC recommended that the Office of the Commonwealth Privacy Commissioner develop and publish guidance on establishing and administering nominee arrangements.<sup>74</sup> It listed a number of issues that the Office of the Commonwealth Privacy Commissioner should address when formulating relevant guidelines including provision for verbal and

---

68. ALRC Report 108, vol 3, [70.7].

69. ALRC Report 108, vol 3, [70.85].

70. ALRC Report 108, vol 3, [70.88].

71. ALRC Report 108, vol 3, [70.8].

72. ALRC Report 108, vol 3, [70.98].

73. ALRC Report 108, Recommendation 70-2.

74. ALRC Report 108, Recommendation 70-3.

written authorisation of nominees; the revocation of nominations; and time limits on nominations.<sup>75</sup>

3.65 The ALRC also recommended that the Office of the Commonwealth Privacy Commissioner provide guidance on other consensual third party arrangements that may assist an individual to make and communicate decisions about his or her privacy, including the use of interpreters, family members, counsellors, and legal representatives.<sup>76</sup> This recommendation was directed towards concerns that agencies and organisations were not recognising instances where individuals were providing consent for the agency or organisation to disclose information to a third party.<sup>77</sup> The ALRC anticipates that guidance on this issue will provide agencies and organisations with the confidence to develop appropriate arrangements that are consistent with the *Privacy Act 1988* (Cth).<sup>78</sup>

3.66 Further, the ALRC recommended against the *Privacy Act 1988* (Cth) giving specific authority to informal representatives—such as family members who do not otherwise have legal authority to make decisions on behalf of an individual with a decision-making disability – to make decisions automatically on behalf of an individual. In the opinion of the ALRC, such authority is already provided for in Australian guardianship and administration regimes and providing such authority in the *Privacy Act 1988* (Cth) could make an individual vulnerable to unacceptable invasions of his or her privacy.<sup>79</sup>

3.67 The ALRC also recommended that agencies and organisations that often handle the personal information of adults with decision-making disabilities ensure that relevant staff are well-informed of issues concerning capacity and are able to recognise and verify the authority of third party agents.<sup>80</sup> It stressed that this does not mean agencies and organisations need to train staff to make an assessment of capacity. This process should be undertaken by professionals consistent with laws and

---

75. ALRC Report 108, vol 3, [70.102].

76. ALRC Report 108, vol 3, [70.8].

77. ALRC Report 108, vol 3, [70.104].

78. ALRC Report 108, vol 3, [70.105].

79. ALRC Report 108, vol 3, [70.6].

80. ALRC Report 108, vol 3, [70.5].

guidelines established by guardianship and administration legislation in each State and Territory.<sup>81</sup>

3.68 The Public Interest Advocacy Centre (“PIAC”) expressed broad support for the ALRC’s recommendations in its submission.<sup>82</sup> PIAC also commented that State legislation with respect to the use of authorised representatives or substitute decision makers should be based upon a uniform Commonwealth model to reflect the fact that guardianship can extend privacy issues beyond and across State borders.<sup>83</sup> PIAC’s proposal has merit and is consistent with our broader recommendation of making NSW privacy law consistent with Commonwealth privacy law. At the time of writing our report, however, the Commonwealth Government had yet to respond to these recommendations of the ALRC.

### The Commission’s view

3.69 In principle, we recognise the need for substitute decision makers and endorse the approach of Privacy NSW in providing for a mixture of substitute and procedural models for determining the capacity of a person with a decision-making disability and for providing consent.

3.70 As to the need for substitute decision makers, we endorse the approach of the ALRC regarding nominee arrangements:

---

#### RECOMMENDATION 3.4

Privacy legislation should provide that an agency may establish nominee arrangements. The agency should then deal with an individual’s nominee as if the nominee were the individual.

---

81. ALRC Report 108, vol 3, [70.121].

82. Public Interest Advocacy Centre, *Submission*, 20.

83. Public Interest Advocacy Centre, *Submission*, 21.

### RECOMMENDATION 3.5

---

Nominee arrangements in privacy legislation should provide at a minimum that:

- (1) an individual or a substitute decision maker authorised by a federal, State or Territory law can make a nomination;
- (2) the nominee can be an individual or an entity;
- (3) the nominee has a duty to act at all times in the best interests of the individual; and
- (4) the individual, the nominee or the agency can revoke the nomination.

3.71 As to providing a mixture of models for determining capacity and providing consent we recommend:

### RECOMMENDATION 3.6

---

The Privacy Commissioner should liaise with the Commonwealth Privacy Commissioner to develop guidelines on obtaining consent from an individual with a decision-making disability. The Privacy Commissioner should review the *Best Practice Guide: Privacy and People with Decision-making Disabilities* with a view to ensuring consistency with any such guidelines.

3.72 It is envisaged that these guidelines will be broad enough to negate the need for separate directions and codes for agencies that regularly deal with individuals with decision-making disabilities. The existence of numerous directions, codes and guidelines, each with different lists of substitute decision-makers and different tests for determining capacity produces unnecessary confusion for substitute decision-makers. The terminology used should also be streamlined so as reduce any confusion that may result from the use of different terms such as “substitute decision-maker” and “authorised representative”. We therefore make the following recommendation:

### RECOMMENDATION 3.7

---

If Recommendation 3.6 is adopted, the guidelines produced by the Privacy Commissioner should be broad enough to negate the need for separate directions and codes for agencies that regularly deal with individuals with decision-making disabilities.

3.73 In making our recommendations, we recognise that several relevant reviews and responses are yet to be released, which are likely to inform future guidelines on how agencies can obtain consent from individuals with decision-making disabilities. The first relevant report is the report of the Standing Committee on Social Issues Committee of the Legislative Council of its inquiry into the provisions for substitute decision-making for people lacking capacity in NSW. The terms of reference require the Committee to inquire into and report on the provisions for substitute decision-making for people lacking capacity in NSW, and in particular whether any NSW legislation should be amended to make better provision for the management of estates of people incapable of managing their affairs and the guardianship of people who have disabilities.<sup>84</sup> The second relevant paper is the Commonwealth Government's response to the ALRC's recommendations in relation to how agencies and organisations can obtain the consent of individuals with decision-making disabilities. The final relevant paper not yet available is the notification statement for individuals with decision-making disabilities that Privacy NSW is developing for agencies in conjunction with NSW Trustee and Guardian (formerly the Office of the Protective Commissioner).<sup>85</sup> In light of the present unavailability of these reviews and papers we make the following recommendation:

#### RECOMMENDATION 3.8

The Privacy Commissioner should develop his or her guidelines in light of the report of the Social Issues Committee of the NSW Legislative Council on the provisions for substitute decision-making for people lacking capacity, the Commonwealth Government's response to the recommendations of the Australian Law Reform Commission and the notification statement produced by the Privacy Commissioner and the NSW Trustee and Guardian.

3.74 We also endorse Recommendation 70-4 of the ALRC that agencies and organisations that regularly handle personal information about adults with limited or no capacity to provide consent should ensure that relevant staff are trained adequately in relation to issues concerning

84. The Standing Committee on Social Issues Committee of the Legislative Council tabled its report on 25 February 2010. This report has not been considered in our report.

85. See Privacy NSW Best Practice Guide, 13.



capacity, and in recognising and verifying the authority of third party representatives.

### RECOMMENDATION 3.9

Agencies that regularly handle personal information about adults with limited or no capacity to provide consent should ensure that relevant staff are trained adequately in relation to issues concerning capacity, and in recognising and verifying the authority of third party representatives.

## YOUNG PEOPLE

### Introduction

3.75 Here we address the question of whether NSW privacy legislation should contain provisions in respect of a person under the age of 18. The issue is particularly important in relation to health information. There is often a contest between a young person's interests in the confidentiality of his or her health information and the interests of parents in the disclosure of that information. In Issues Paper 24 we identified circumstances in which the law concerning permissible disclosure of a young person's health information may need reform, including when parents request disclosure of their child's health information; when the consent of the young patient renders disclosure permissible; when disclosure is authorised by HRIPA; and when the public interest in preventing harm to a young person requires disclosure.<sup>86</sup> We preferred, however, to leave our final recommendations on these issues to this report.<sup>87</sup>

### Current framework

#### *PPIPA and HRIPA*

3.76 PPIPA is silent as to whether a person under the age of 18 years can provide the requisite consent for the purposes of the Act. Section 9, however, provides that a public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless the individual is aged under 16 years and a

---

86. NSW Law Reform Commission, *Minors' Consent to Medical Treatment*, Issues Paper 24 (2004), Chapter 9.

87. NSWLRC Report 119, [1.64].

parent or guardian of the individual has authorised collection of the information.

3.77 Similarly, HRIPA does not specify whether a person under the age of 18 years is capable of providing consent for the purposes of the Act. In fact, it is unclear from the Act what the position of young people is in regards to the issue of consent. Paragraph 8(1)(c) sets out that an “authorised representative” in relation to an individual means a person having parental responsibility for the individual, if the individual is a child. Sub-section 8(3) defines “child” to mean an individual under 18 years of age and defines “parental responsibility”, in relation to a child, to mean all the duties, powers, responsibility and authority which, by law, parents have in relation to their children. Paragraph 9(b) provides that a public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless information has been provided by a parent or guardian of a person who is under the age of 16 years.

#### *Privacy codes and directions*

3.78 The *Privacy Code of Practice: Department of Education and Training 2000* modifies a number of the IPPs that apply to certain functions of the Department of Education and Training (DET). The code clarifies who may provide the requisite consent in relation to the collection, use and disclosure of a young person’s personal and sensitive information. For example, cl 4.3.2 provides that the DET may depart from s 9 of PPIPA to allow the collection of personal information about a student at a government school from the parent, guardian or caregiver of the student. The code also recognises the autonomy of young people in some situations. For instance, cl 3.2 sets out that where a student objects to a decision concerning his or her personal information (for example, he or she does not wish to have his or her personal information disclosed to a parent, guardian or caregiver) that decision is to be reviewed by the principal of the school, with a right of appeal to the district superintendent. However, the code also potentially restricts the ability of a young person to play an active role in determining how his or her information will be handled. For example, cl 4.5.2 allows the DET to depart from s 14 in certain circumstances, by allowing the DET to seek the approval of the parent, guardian or caregiver of a student before the DET releases personal information to a student enrolled at a government school.

3.79 There are several public interest directions that recognise the capacity of a child to provide the requisite consent under the direction.<sup>88</sup> For example, the “Direction relating to the Redfern Waterloo Partnership Project”<sup>89</sup> establishes a case co-ordination framework pursuant to which a contact agency assesses whether it is appropriate to refer a young person to a Redfern/Waterloo Case Coordination Senior Officers’ Group (“RWCCSOG”). If the agency concludes that an individual should be so referred, then it must determine whether it is in the best interests of the individual and/or the public interest to obtain the consent of the individual (or, where appropriate, a parent or guardian) to refer his or her case to the RWCCSOG.<sup>90</sup>

## Submissions

3.80 There was support in the submissions for young people to be able to provide consent under privacy legislation.<sup>91</sup> There was also support for the proposal<sup>92</sup> that HPP 3 be amended to allow collection of information about an individual under the age of 16 years from a parent or guardian.<sup>93</sup>

## The approach of the ALRC

3.81 There is no Commonwealth legislation specifically addressing the privacy of young people. In response to this legislative gap, the ALRC recommended that the *Privacy Act 1988* (Cth) be amended to provide that an assessment about the capacity of an individual under the age of 18 to give consent, make a request or exercise a right of access under the Act, should be undertaken where it is reasonable and practicable to do so. The recommendation was made after a consideration of the research on the

---

88. See, for example, the NSW Privacy Commissioner, “Direction relating to the Anti-Social Behaviour Pilot Project”, Public Interest Direction (2 September 2008) and the NSW Privacy Commissioner, “Direction relating to the Redfern Waterloo Partnership Project”, Public Interest Direction (2 February 2006).

89. NSW Privacy Commissioner, “Direction relating to the Redfern Waterloo Partnership Project”, Public Interest Direction (2 February 2006).

90. See also the “Operation of the Case Coordination Guidelines” in NSW Privacy Commissioner, “Direction relating to the Anti-Social Behaviour Pilot Project”, Public Interest Direction (2 September 2008).

91. NSW Department of Education and Training, *Submission*, 4.

92. NSWLRC CP 3, Proposal 9.

93. Cyberspace Law and Policy Centre, *Submission*, 20; NSW Department of Education and Training, *Submission*, 4; Public Interest Advocacy Centre, *Submission*, 20.

decision-making capacity of young people, international law and recent case law, all of which support an individual assessment of capacity.<sup>94</sup> It was noted that the recommendation was consistent with other privacy legislation in Australia and had received strong community support during the ALRC's consultation process. The ALRC envisaged that an assessment would involve communicating with a young person to enable him or her to understand the nature and consequences of a decision.<sup>95</sup>

3.82 The ALRC recognised, however, that the proposed model is subject to practical difficulties and limitations. For example, the model presupposes that it is possible to engage with the individual and requires that the person making the assessment has the skills and qualifications necessary to make an appropriate judgement about the capacity of the individual. It is possible, however, that these requirements may not be easily met in some situations. For instance, it may not be possible to engage with an individual at the level required where an agency is conducting a survey over the telephone and the survey involves disclosing sensitive personal information.

3.83 In light of these limitations, the ALRC recommended that where an assessment of capacity is not reasonable or practicable, then an individual aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access; and an individual under the age of 15 is presumed to be incapable of giving consent, making a request or exercising a right of access.<sup>96</sup> It also recommended that the *Privacy Act 1988* (Cth) be amended to provide that, in order to rely on the age-based presumption, an agency or organisation is required to take such steps, if any, as are reasonable in the circumstances to verify that the individual is aged 15 or over.<sup>97</sup> The age of 15 years was selected by the ALRC in light of the latest research on child development and the brain development of adolescents and community debates about ages of capacity.<sup>98</sup>

3.84 The ALRC also recommended that amendments be made to the *Privacy Act 1988* (Cth) so that where an individual under the age of 18 is assessed or presumed to not have capacity under the Act, any consent,

---

94. ALRC Report 108, vol 3, [68.25]-[68.42].

95. ALRC Report 108, vol 3, [68.54].

96. ALRC Report 108, vol 1, Recommendation 68-1.

97. ALRC Report 108, vol 1, Recommendation 68-3.

98. See generally ALRC Report 108, vol 3, Chapter 68.

request or exercise of a right in relation to that individual must be provided or made by a person with parental responsibility for the individual.<sup>99</sup> The ALRC, unfortunately, did not consider the situation of young people, such as homeless youth, who may not have a person (or access to a person) who has responsibility for him or her.

3.85 The ALRC also recommended that the Office of the Commonwealth Privacy Commissioner develop and publish guidance for applying the new provisions of the *Privacy Act 1988* (Cth) relating to individuals under the age of 18. The areas on which the Office of the Commonwealth Privacy Commissioner could provide guidance include situations in which it is reasonable and practicable to make an assessment regarding the capacity of a young person and what an agency could reasonably do to assist a young person to understand and communicate decisions.<sup>100</sup>

### The Commission's view

3.86 We make the following recommendations with regard to young people:

#### RECOMMENDATION 3.10

Privacy legislation should provide that an agency is to assess the capacity of an individual under the age of 18 to give consent where it is reasonable and practicable to do so.

3.87 This recommendation is consistent with the recommendations we made in Report 119,<sup>101</sup> the ALRC's recommendations, the approach at common law and the suggestions made by stakeholders.<sup>102</sup> It would also meet the desires of young people who wish to be involved in decisions about what information is collected about them, how it is collected and to whom it is released.<sup>103</sup> It would also go some way to addressing the problem PIAC identified in its submission, namely, that of individuals

99. ALRC Report 108, Recommendation 68-6.

100. ALRC Report 108, Recommendation 68-4.

101. See, for example, NSWLRC Report 119, Recommendation 4.

102. NSW Commission for Children and Young People, *Submission*, 4.

103. NSW Commission for Children and Young People, *Submission*, 2.

under the age of 16 who have not disclosed all of their personal information to their parents or guardian.<sup>104</sup>

### RECOMMENDATION 3.11

---

Privacy legislation should provide that where an assessment of capacity is not reasonable or practicable, then an individual aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access.

3.88 We acknowledge that there are persuasive reasons for making the presumption dependent on the nature of the personal information involved, given that decisions regarding certain types of information may involve complex factors and serious consequences. However, this approach is likely to cause some confusion for agencies, organisations and individuals, and we are of the view that a less complex approach is preferable.

3.89 We also acknowledge that in Report 119, we recommended a presumption that young people aged 16 and over are competent to consent to or refuse health care, whereas in this report, we have recommended an age of 15 years at which it can be presumed that a young person has the capacity to provide the requisite consent for the purposes of privacy legislation. This inconsistency is not a substantial one. This is because decisions to allow or refuse health care can have consequences that are more long-term and far-reaching than decisions concerning the use of personal and sensitive information. There was no particular age suggested in the submissions we received, although there was support for informed 15 or 16 year olds being able to make their own decisions with respect to the use of their information.<sup>105</sup> Further, the presumptions in our recommendation and the ALRC's recommendation are only used where an individual assessment is not possible.

### RECOMMENDATION 3.12

---

Where a young person is found to lack the capacity to consent to particular medical treatment but can comprehend an obligation of secrecy with

---

104. Public Interest Advocacy Centre, *Submission*, 20.

105. Cyberspace Law and Policy Centre, *Submission*, 20.

respect to health information obtained by the medical practitioner, the fact that he or she consulted the medical practitioner, and what the medical practitioner has learned in the process of assessing competence to consent to that particular treatment, must not be disclosed if the young person:

- (a) expressly objects to the disclosure; or
- (b) gave the information with an expectation that it would not be disclosed.

3.90 This recommendation recognises the autonomy of young people and young people's needs for privacy, which should not be less than those of adults. It also encourages the effective delivery of health services because, without the guarantee of confidentiality, many young people will not seek medical advice or treatment.<sup>106</sup> It is consistent with the views expressed in submissions and consultations we received when undertaking our inquiry for Report 119, which (with exceptions relating to mandatory reporting laws) argued that medical practitioners should generally respect the confidentiality of information that young people disclosed to them in the course of a medical consultation or proposed medical treatment whether or not the young person was competent to consent to that treatment.<sup>107</sup>

3.91 Importantly, our recommendations should not be regarded as overriding existing laws as to confidentiality and exceptions to confidentiality, such as s 27 of the *Children and Young Persons (Care and Protection) Act 1998* (NSW) which provides that medical practitioners (among others) must report to the Director-General of the Department of Youth and Community Services, the name or a description of the child and the grounds for suspecting that the child is at risk when they have reasonable grounds to suspect that a child is at risk of harm, and those grounds arise during the course of or from their work.

#### RECOMMENDATION 3.13

Agencies and organisations that regularly handle the personal information of individuals under the age of 18 should have privacy policies that address how such information is managed and how the agency or organisation will determine the capacity of individuals under the age of 18. Such agencies

106. NSWLRC Report 119, [1.60].

107. NSWLRC Report 119, [1.63].

and organisations should also ensure that relevant staff are trained about issues concerning capacity, including when it is necessary to deal with third parties on behalf of those individuals.

3.92 This recommendation includes “organisations” because HRIPA applies to every organisation that is a health service provider or that collects, holds or uses health information.<sup>108</sup>

3.93 This recommendation is important in light of the concerns expressed by the Shopfront Youth Legal Centre that young people have experienced difficulty in circumstances where health service providers have not recognised that a young person who has the requisite capacity is able to provide the relevant consent for accessing his or her health information without parental consent or knowledge.<sup>109</sup> Proper training may also go some way to addressing the observation of the NSW Commission for Children and Young People that the ability of young people to receive the services of agencies is often made difficult by the differing views and misunderstandings that individual agencies have about the operation of the various privacy laws.<sup>110</sup>

---

108. *Health Records and Information Privacy Act 2002* (NSW) s 11. Note however that we have recommended the repeal of HRIPA: Recommendation 1.1.

109. The Shopfront Youth Legal Centre, *Preliminary Submission*, 3.

110. NSW Commission for Children and Young People, *Submission*, 1.



## 4. Exemptions for lawful non-compliance

- Introduction
- Lawful non-compliance
- Defining “law” for the purposes of the exemption
- A particular problem: preliminary inquiries

## INTRODUCTION

### What the chapters on exemptions cover

4.1 This chapter, and the following four chapters, deal with situations in which agencies are exempt from complying with privacy principles or other provisions of the *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”) and the *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”).<sup>1</sup> Such exemptions may arise from a number of sources:

- by virtue of definitions contained in PPIPA and HRIPA;<sup>2</sup>
- “specific exemptions from principles”;<sup>3</sup>
- special exemptions contained in PPIPA and HRIPA;<sup>4</sup>
- in regulations;<sup>5</sup>
- pursuant to privacy codes of practice;<sup>6</sup> and
- pursuant to public interest directions.<sup>7</sup>

- 
1. In its final report on privacy, the ALRC highlighted a distinction in terminology where a privacy principle does not apply. The ALRC distinguished between exemptions, partial exemptions and exceptions. The same distinction is often made by the ADT. In this report, we use the terms “exemption” and “exception”. The distinction is terminological, and, in practice exemptions and exceptions operate in a similar manner. We use “exemption” where a specified entity or a class of entity is not required to comply with either: all of the provisions of privacy legislation; some, but not all, of the provisions of privacy legislation; or some or all of the provisions of privacy legislation, but only in relation to particular activities. We use “exception” where a requirement in the privacy principles does not apply to any entity in a specified situation or in respect of certain conduct. See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”) vol 2, [33.1]-[33.2].
  2. *Privacy and Personal Information Protection Act 1998* (NSW) s 4, s 4A; *Health Records and Information Privacy Act 2002* (NSW) s 5, s 6.
  3. *Privacy and Personal Information Protection Act 1998* (NSW) pt 2 div 3; *Health Records and Information Privacy Act 2002* (NSW) s 17 and sch 1.
  4. *Privacy and Personal Information Protection Act 1998* (NSW) s 6, s 20(5); *Health Records and Information Privacy Act 2002* (NSW) s 13, s 14, s 22.
  5. See para 7.4-7.14.
  6. *Privacy and Personal Information Protection Act 1998* (NSW) pt 3 div 1. See para 7.15-7.65.

4.2 Chapters 4-6 deal with specific exemptions and special exemptions. Exemptions created by regulations, privacy codes or public interest directions are dealt with in chapter 7. Chapter 8 discusses how privacy legislation should apply to public registers.

### What the chapters do not cover

4.3 This chapter does not deal with exemptions arising out of definitions. Exclusion from the ambit of PPIPA is not limited to express exemption contained in the legislative provisions. Exemptions also occur by virtue of definitions. For example, the definition of a “public sector agency” currently excludes state owned corporations and perhaps other bodies that are not expressly described as “a statutory body representing the Crown”.<sup>8</sup> Chapter 2 addresses the adequacy of the current definition of “public sector agency”.<sup>9</sup>

4.4 Since PPIPA only applies to “personal information”, the requirements of the Act do not apply to information excepted from the definition of “personal information” in s 4.<sup>10</sup> We have considered these exceptions in our report, *Access to Personal Information*, where we have recommended that all the exceptions contained in s 4(3) be removed, except s 4(3)(a) and s 4(3)(k).<sup>11</sup>

### The differing approaches in PPIPA, HRIPA and the UPPs

4.5 The Information Protection Principles (“IPPs”) found in PPIPA apply to public sector agencies.<sup>12</sup> Health Privacy Principles (“HPPs”) found in HRIPA apply to “organisations”, that is, public sector agencies or a private sector person.<sup>13</sup> Public sector agencies may not be required to comply with these principles if they are able to satisfy one of the many exemptions found within PPIPA or HRIPA.

---

7. *Privacy and Personal Information Protection Act 1998* (NSW) s 41. See para 7.66-7.91.

8. See para 2.1-2.26; *Privacy and Personal Information Protection Act 1998* (NSW) s 3(1).

9. See Recommendations 2.1-2.6.

10. *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3) contains a long list of exceptions to the definition of “personal information”.

11. NSW Law Reform Commission, *Access to Personal Information*, Report 126 (2009) Recommendation 9.

12. *Privacy and Personal Information Protection Act 1998* (NSW) s 20(1).

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

4.6 There is a great deal of concern about the operation of the exemptions in privacy legislation. For example, the exemptions are not contained together in PPIPA, but are instead to be found in various places throughout the Act. Consequently, it is difficult for public sector agencies to determine whether a particular act or practice qualifies for exemption. These fragmented and confusing exemption mechanisms need amending to bring some clarity and transparency to the operation of privacy legislation.

4.7 Under HRIPA, although there are some “specific” and “special” exemptions listed, most of the exemptions are contained within the HPPs. The approach adopted under HRIPA is different to that under PPIPA and is arguably much clearer. As HRIPA was drafted some years after PPIPA, it was able to benefit from the experience of problems that had arisen under PPIPA.

4.8 The exemptions under the proposed Unified Privacy Principles (“UPPs”) operate in a similar way to HRIPA. The UPPs contain a number of exceptions to each privacy principle. These exceptions, as well as the principles themselves, are broadly formulated so as to contemplate a wide range of circumstances where compliance with the relevant privacy principle would be inappropriate.

### The Commission’s approach

4.9 We recommended in an earlier Report that the proposed UPPs be adopted in NSW.<sup>14</sup> The exceptions contained within the UPPs would significantly overlap with the exemptions currently found in PPIPA and HRIPA. Throughout this and subsequent chapters, we review the extent to which the current exemptions under PPIPA and HRIPA are covered by the proposed UPPs. Additionally, we question the appropriateness of the current level of exemption under PPIPA and HRIPA and review whether additional exemption from the UPPs is warranted.

4.10 In the event that the UPPs are not adopted in NSW, we provide a number of recommendations relating to the exemptions under PPIPA, and to a much lesser extent under HRIPA. Given the concerns expressed

---

14. See NSW Law Reform Commission, *Privacy Principles*, Report 123 (2009) (“NSWLRC Report 123”) where we recommended several modifications to the UPPs.

by many stakeholders, we examine the current structure, scope and clarity of the exemptions.

4.11 The uniform national scheme of privacy law recommended by the Australian Law Reform Commission (“ALRC”) and supported by us,<sup>15</sup> may result in the repeal of HRIPA.<sup>16</sup> This means that health information not regulated by the *Privacy Act 1988* (Cth) will be regulated under PPIPA. If the uniform scheme is not adopted and HRIPA remains in force, the recommendations in respect of the exemptions under PPIPA will need to be consistently applied, where necessary, to the exemptions under HRIPA.

## LAWFUL NON-COMPLIANCE

### The rationale of a lawful non-compliance exemption

4.12 An agency will not be required to comply with certain privacy principles if non-compliance is required, authorised or permitted under another law. This provides a necessary exemption to agencies. It is important to enable governments to perform their functions, especially in areas of law enforcement and national security. The NSW Department of Corrective Services has highlighted the necessity for privacy protection to be limited where compliance with privacy laws would result in an agency being unable to carry out the functions, powers and duties conferred on them by Parliament, including those relating to the maintenance of security and order in correctional facilities and the effective and efficient management of orders and sentences served in the community.<sup>17</sup>

4.13 This exemption may also subsume more specific exemptions – for example, in relation to investigations – if an agency has lawful authorisation, or is lawfully required, to perform an act or practice that may be subject to privacy principles.

---

15. NSWLRC Report 123.

16. See Recommendation 1.1.

17. NSW Department of Corrective Services, *Submission to NSW Law Reform Commission Consultation Paper 1: Invasion of Privacy* (12 October 2007). Similarly, the Department of Education and Training has stated that it is vital to their role that privacy legislation does not prevent agencies from complying with law, including common law: NSW Department of Education and Training, *Submission*, 7-8.

## The differing approaches in PPIPA, HRIPA and the UPPs

4.14 The approach taken under PPIPA is different from that taken under HRIPA and the proposed UPPs. Under PPIPA, there is a specific exemption in s 25 which lists a number of IPPs that an agency may not need to comply with. Under HRIPA and the proposed UPPs, there are a number of HPPs and UPPs that contain a lawful non-compliance exception to a single privacy principle.

### PPIPA

4.15 Pursuant to s 25 of PPIPA, an agency is not required to comply with s 9, s 10, s 13, s 14, s 15, s 17, s 18 and s 19 of PPIPA if:<sup>18</sup>

- the agency is lawfully authorised or required not to comply with the principle concerned; or
- non-compliance is otherwise permitted under an Act or any other law.

4.16 There are three ways that non-compliance with an IPP can be achieved under s 25. Another law can “require” or “authorise” non-compliance<sup>19</sup> or “otherwise permit” non-compliance. An act or practice is “required” when the law in question “demands” or “necessitates” that it be undertaken,<sup>20</sup> a common example being a legislative requirement on a defendant to disclose personal information.<sup>21</sup> In contrast, an act or practice is “authorised” when the law in question permits it to be done but leaves it up to the person concerned to decide whether or not he or she will do it. An act or practice is not, however, “authorised” simply because there is no law prohibiting it.<sup>22</sup>

4.17 The phrase “otherwise permit” is used in PPIPA along with “or is necessarily implied or reasonably contemplated”. The Administrative Decisions Tribunal (“ADT”) has held that the phrase is “extremely broad”.<sup>23</sup> It applies where another law implies or reasonably

---

18. HPPs 4(4)(b), 5(2)(a), 6(2)(a), 7(2)(a), 8(4)(a), 10(2)(a), 11(2)(a) and 15(2)(a); *Health Records and Information Privacy Act 2002* (NSW) s 23.

19. See ALRC Report 108, vol 1, [16.2]-[16.26].

20. See, eg, *Secretary to the Department of Premier and Cabinet v Hulls* [1999] 3 VR 331, [358] (Phillips JA).

21. See, eg, *Rahman v Ashpole* [2007] FCA 1067.

22. See, eg, *Caratti v Commissioner of Taxation* (1999) 99 ATC 5044, [27] (French J).

23. *JS v Snowy River Shire Council (No 2)* [2009] NSWADT 210, [53].

contemplates that compliance with a privacy principle is not required. If another law requires or authorises a disclosure of personal information, then this law would permit non-disclosure and thus an agency need not comply with disclosure principles.

4.18 Submissions thought that s 25 is unclear, leaving agencies unsure as to when they are required to comply with a privacy principle. This section gives rise to the following difficulties:

- (1) It is arguable that s 25(a) of PPIPA is limited to statute law because it is difficult to understand how an agency could otherwise be lawfully authorised or required not to comply with one of the specific IPPs (except, perhaps, impliedly). The wording of this section is strict in that, on one interpretation, it must be non-compliance with the relevant principle that needs to be “required or authorised”.
- (2) It is unclear whether “permitted” in s 25(b) allows anything that is not prohibited. The extent to which PPIPA limits this construction by referring to “necessarily implied” or “reasonably contemplated” is also unclear. The problem, therefore, is that deference can be accorded to other Acts or laws which may “permit” non-compliance. Some stakeholders argued that s 25(b) should be repealed in that it is too vague and uncertain.<sup>24</sup>
- (3) The reference in s 25(b) to “any other laws” has caused problems as to whether “law” here includes common law, or, for example, court rules.<sup>25</sup> This ambiguity is a problem experienced in other jurisdictions, where privacy legislation is similarly worded.<sup>26</sup> The ADT has favoured a broad interpretation of this section which encompasses common law. In *Director General, Department of Education and Training v MT*, for example, it was held that the circumstances in that case gave rise to a duty to warn – a common law obligation –

---

24. Australian Privacy Foundation, *Submission*, 12; Cyberspace Law and Policy Centre, *Submission*, 28; Public Interest Advocacy Centre, *Submission*, 26.

25. *Re An Application by the NSW Bar Association* [2004] FMCA 52; *GV v Office of the Director of Public Prosecutions* [2003] NSWADT 177.

26. See the *Information Privacy Act 2000* (Vic) sch 1 IPP 2.1(f); see also ALRC Report 108, vol 1, [16.20]-[16.47].

and thus fell “within the scope of the expression ‘any other law’”.<sup>27</sup> Other examples include personal information disclosed pursuant to a common law obligation of procedural fairness<sup>28</sup> and a subpoena.<sup>29</sup> Submissions were divided on how the definition of “law” should be clarified: some were in support of adopting the ADT’s broader approach so as to include common law duties;<sup>30</sup> on the other hand, there was support for a narrower construction limited to statutes.<sup>31</sup>

## HRIPA and the proposed UPPs

4.19 HRIPA covers similar privacy principles to PPIPA and the exemption is similarly worded. However the exemption operates in a different way. HPPs 4(4)(b), 5(2)(a), 6(2)(a), 7(2)(a), 8(4)(a), 10(2)(a), 11(2)(a) and 15(2)(a) have self-contained exemptions. Most of these are equivalent to the exemptions provided under s 25 of PPIPA, however HPP 5(2)(a) and 15(2)(a) do not have an equivalent under PPIPA.

4.20 The proposed UPPs have self-contained “required or authorised by or under law” exemptions. However, the language differs from that used in s 25 of PPIPA. UPPs 2 (Collection), 5 (Use and Disclosure), 8 (Data Security), 9 (Access and Correction) and 11 (Cross-Border Data Flows) contain certain exceptions to the requirements of each UPP where the use or disclosure, for example, is “required or authorised by or under law”.<sup>32</sup>

---

27. *Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77, [83].

28. *KD v Registrar, NSW Medical Board* [2004] NSWADT 5, [32]-[34].

29. *HW v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 214, [64].

30. Guardianship Tribunal, *Submission, 2*; NSW Department of Education and Training, *Submission, 8*; NSW Department of Corrective Services, *Submission to NSW Law Reform Commission Consultation Paper 1: Invasion of Privacy* (12 October 2007) 3.

31. Australian Privacy Foundation, *Submission, 12*; Cyberspace Law and Policy Centre, *Submission, 28*; Inner City Legal Centre, *Submission, 18*; Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 89; see also comments of the Privacy Commissioner in *MT v Director General, NSW Department of Education and Training* [2004] NSWADT 194, [143].

32. UPP 3 (Notification) also requires that an agency or organisation must notify an individual of the fact that the collection is required or authorised by or under law.



These would cover s 9, s 10, s 17, s 18 and s 19 listed in s 25.<sup>33</sup> The other mentioned IPPs in s 25 (s 13, s 14 and s 15) would be covered by the qualifications to the equivalent UPP 9 (Access and Correction).<sup>34</sup>

4.21 It is of significance that the wording used in the proposed UPPs differs from that used in s 25 of PPIPA and in the HPPs. The test under UPP 5.1(e), for example, is whether “the use or disclosure is required or authorised by or under law”. The requirements of this test are clearer than those in s 25(a), where it must be the non-compliance which needs to be “required or authorised”. This, and the absence of the term “permitted”, avoid difficulties (1) and (2) identified in para 4.18.

### The Commission’s view

4.22 We are satisfied that the adoption of the UPPs in NSW would sufficiently fulfil the purpose of s 25. Consequently, we recommend that s 25 be repealed. We note that the UPPs do not contain the broader provision found in s 25(b). However, for the reasons outlined below, we do not regard this as problematic.<sup>35</sup>

---

#### RECOMMENDATION 4.1

If the UPPs are adopted in NSW, s 25 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

#### *If the UPPs are not adopted in NSW*

4.23 If the proposed UPPs are not adopted in NSW, s 25 should be amended to resolve its ambiguity. We recommend that s 25 should be amended so as to have a single “required or authorised by or under law” exemption to certain IPPs.

4.24 We recommend that s 25(b) should be repealed to make it clear that the other law being relied upon must authorise or require non-compliance. This would achieve a single “required or authorised by law”

---

33. They would also cover HPPs 4(4)(b), 5(2)(a), 10(2)(a) and 11(2)(a).

34. See NSWLRC Report 123, Chapter 9 generally. UPP 9 would also cover HPPs 6(2)(a), 7(2)(a) and 8(4)(a). HPP 15(2)(a) is not specifically addressed in the UPPs.

35. See para 4.24-4.25.

exemption from the principles currently listed in s 25.<sup>36</sup> To avoid confusion, this exemption should specify that the agency can be either expressly or impliedly required or authorised not to comply with a privacy principle. Some laws may not expressly state that an act or practice needs to comply with a privacy principle, although it is implied in the law that non-compliance is required or authorised.

4.25 In removing the “otherwise permitted (or is necessarily implied or reasonably contemplated)” test, s 25 will no longer be as broad or vague as to the extent to which another law permits non-compliance with certain IPPs. The extent of non-compliance should be narrowly limited to what the other law requires or authorises (whether expressly or impliedly).<sup>37</sup> Thus, if another law requires or authorises an act or practice, this act or practice need not comply with the relevant privacy principle.

#### RECOMMENDATION 4.2

If the UPPs are not adopted in NSW:

- (1) s 25(b) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed; and
- (2) s 25(a) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to exempt an agency from compliance with a relevant IPP when non-compliance is required or authorised (whether expressly or impliedly) by or under law.

### DEFINING “LAW” FOR THE PURPOSES OF THE EXEMPTION

4.26 Even if the approach in the proposed UPPs is adopted, it is essential to understand what “law” means for the purposes of the exemption. In Report 120 we addressed this issue in the context of a statutory cause of action for invasion of privacy, and recommended a

36. We note that under *Health Records and Information Privacy Act 2002* (NSW) there is the additional exemption from the retention and security HPP 6. If HRIPA is not repealed (see Recommendation 1.1), *Privacy and Personal Information Protection Act 1998* (NSW) s 25 should be amended to include exemption from s 12.

37. *ZR v NSW Department of Education and Training* [2009] NSWADT 84, [47].

broad definition.<sup>38</sup> The ALRC has reviewed this issue and recommended that, given the ambiguity, the term “law” be defined for the purposes of the “required or authorised by or under law” exceptions in the *Privacy Act 1988* (Cth). The ALRC supported a broad definition of “law”, suggesting that it include:

- Commonwealth, State and Territory Acts and delegated legislation;
- a duty of confidentiality under common law or equity (including any exceptions to such a duty);
- an order of a court or tribunal; and
- documents that are given the force of law by an Act, such as industrial awards.<sup>39</sup>

4.27 The ALRC was of the view that including other common law duties in the definition may be difficult and have unintended consequences.<sup>40</sup> It recommended that, rather than rely on the common law generally, particular common law and equitable duties (and exceptions to those duties) ought to be specified.<sup>41</sup> It further suggested that other common law duties, such as a school’s duty of care or a duty to accord procedural fairness, may be relevant and, depending on the circumstances of the case, may “be caught by the term ‘law’ for the purposes of the required or authorised exception”.<sup>42</sup>

4.28 In its response to the ALRC, the Commonwealth Government has commented that, while it accepts in principle the ALRC’s definition, it preferred a broader reference to “common law or equitable duties”, rather than merely “duties of confidentiality”.<sup>43</sup> A case-by-case development was preferred.

---

38. NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) (“NSWLRC Report 120”) [6.3]-[6.5].

39. ALRC Report 108, vol 1, Recommendation 16-1.

40. ALRC Report 108, vol 1, [16.64].

41. ALRC Report 108, vol 1, [16.64].

42. ALRC Report 108, vol 1, [18.67].

43. Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice* (2009) 34.

## The Commission's view

4.29 In the interests of clarity, we recommend that the term “law” be defined for the purposes of s 25. We are of the view that a broad definition of “law” is warranted, not confined to statutes as submitted by some stakeholders.<sup>44</sup> The wider view is generally consistent with the ALRC’s recommendation,<sup>45</sup> our view in Report 120,<sup>46</sup> and the response of the Commonwealth Government.<sup>47</sup>

4.30 In particular, we regard the following as falling within the meaning of “law”:

- Other Acts (whether NSW or Commonwealth) including delegated legislation. These types of law will provide circumstances where Parliament has deemed it appropriate to render privacy requirements inapplicable. They have the benefit of being subject to review and debate.
- Documents given legal authority under an Act. The provision being relied upon under the relevant Act will need to be examined to ascertain whether the secondary document was intended to have the force of law. As the ALRC has identified, industrial awards may fall under this category.<sup>48</sup>
- Orders of courts and tribunals. Orders for discovery or a subpoena, although affecting privacy, may be necessary to ensure that justice is administered effectively.

---

44. Cyberspace Law and Policy Centre, *Submission*, 28; Australian Privacy Foundation, *Submission*, 12.

45. ALRC Report 108, vol 1, Recommendation 16-1.

46. NSWLRC Report 120, [6.5] where we recommended that “law” for the purposes of the Civil Liability Amendment (Privacy) Bill 2009 should include common law, but did not specify, as the ALRC did, the types of common law.

47. Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice* (2009) 40.

48. ALRC Report 108, vol 1, [16.70]. Other decisions made under a power may also be relevant. For example, the *Workplace Surveillance Act 2005* (NSW) s 41 grants a power to a judicial member of the Industrial Relations Commission “to issue, vary or cancel the [covert surveillance] authority” where an applicant is aggrieved by the decision of a Magistrate. Section 26 also requires that privacy be a consideration in determining whether to issue an authority. This award could permit workplace surveillance and hence infringe privacy principles.

- A duty of confidentiality at common law or in equity. Explicitly recognising duties of confidentiality (and exceptions to those duties) will ensure that entrenched professional practices are allowed to continue,<sup>49</sup> satisfying the concerns of professionals, particularly the medical profession.<sup>50</sup>
- Other common law duties, such as duty of care, should fall within “law” in appropriate factual circumstances.<sup>51</sup> Notwithstanding that such duties may not be readily ascertainable, they are nevertheless important. For example, a school will owe a duty of care to take safety precautions in relation to a child while at school, because of “the need of a child of immature age for protection against the conduct of others, or indeed of himself, which may cause him [or her] injury coupled with the fact that, during school hours the child is beyond the control and protection of his [or her] parent and is placed under the control of the schoolmaster who is in a position to exercise authority over him [or her]”.<sup>52</sup> Thus there may be a positive duty required of schools to take action to protect the welfare of a child. This duty may require non-compliance with a privacy principle, and, accordingly, should be the basis for an exemption.
- Case law has recognised that procedural fairness may, in some cases, require a relaxation of privacy principles. As is now well established in the common law, “when an order is to be made which will deprive a person of some right or interest or the legitimate expectation of a benefit, he is entitled to know the case sought to be made against him and to be given an opportunity of

---

49. For, as has been said in the context of confidentiality in conciliation, “in this field as in others it is undesirable that the law should drift very far away from the best professional practice”: *In Re D. (Minors)* [1993] Fam 231, 235 (Sir Thomas Bingham MR).

50. ALRC Report 108, vol 1, [16.34].

51. ALRC Report 108, vol 1, [16.66]. We acknowledge that one of the problems in relying on a case by case assessment in determining whether the duty is “law” for the purposes of the *Privacy and Personal Information Protection Act 1998* (NSW) that “[t]o make findings of this kind, there would, we think, virtually have to be a trial within a trial. The relevant law is multi-factored; and the evidentiary requirements are substantial”: *Director General, Department of Education and Training v MT* (2006) 67 NSWLR 237, 248.

52. *Richards v State of Victoria* [1969] VR 136, 138 (Winneke CJ).

replying to it”.<sup>53</sup> In instances of a complaint, this will place a duty upon the decision maker to disclose the substance of allegations made against a person to allow them to respond.<sup>54</sup> For example, in relation to an investigation by the NSW Medical Board into a complaint made against Dr A, the ADT stated that “[i]t is difficult to see how the investigation could proceed without the disclosure of [the] document ... as a matter of procedural fairness the Board had no option but to disclose it to Dr A”.<sup>55</sup> This should be the basis of an exemption. Where this is so, suitable responses can be devised, for example, by requiring that the *substance* of a complaint be disclosed.<sup>56</sup> As with the duty of care, we acknowledge that the scope and requirements of procedural fairness will depend upon the facts and circumstances of each case as to what is required to fulfil this duty.<sup>57</sup>

4.31 We are of the view that it is unnecessary to limit the scope of common law for the purposes of the exemption. We are of the view that the definition of “law” should include “common law” and “equity”, which would include all of the relevant duties applicable to agencies.

---

53. *Kioa v West* (1985) 159 CLR 550, 582 (Mason J).

54. *Applicant VEAL of 2002 v Minister for Immigration and Multicultural and Indigenous Affairs* (2005) 225 CLR 88; in the context of PPIPA see: *KD v Registrar, NSW Medical Board* [2004] NSWADT 5.

55. *KD v Registrar, NSW Medical Board* [2004] NSWADT 5, [36].

56. *Applicant VEAL of 2002 v Minister for Immigration and Multicultural and Indigenous Affairs* (2005) 225 CLR 88; in the context of the *Privacy and Personal Information Protection Act 1998* (NSW) see *KD v Registrar, NSW Medical Board* [2004] NSWADT 5.

57. *SZBEL v Minister for Immigration and Multicultural and Indigenous Affairs* (2006) 228 CLR 152, 160-161; see also *Applicant VEAL of 2002 v Minister for Immigration and Multicultural and Indigenous Affairs* (2005) 225 CLR 88.

### RECOMMENDATION 4.3

For the purposes of an exemption in privacy legislation referable to non-compliance required or authorised by or under law (as in s 25(a) of the *Privacy and Personal Information Protection Act 1998* (NSW)) "law" should be defined to include:

- NSW law or Commonwealth law;
- an order of a court or tribunal;
- documents that are given the force of law by an Act; and
- common law and equity.

## A PARTICULAR PROBLEM: PRELIMINARY INQUIRIES

4.32 There have been further concerns as to the scope of s 25(b) in respect of its application to preliminary inquiries by the Ombudsman. The Ombudsman, as the State's main complaints handling body, conducts preliminary inquiries into a complaint prior to conducting a formal investigation. This is for the purposes of determining a complaint's prima facie merit and encouraging informal resolution.

4.33 Section 13AA(1) of the *Ombudsman Act 1974* (NSW) provides that:

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.

The Ombudsman has received advice that this section is not sufficient to enliven s 25(b) of PPIPA.<sup>58</sup> Consequently, agencies are prevented from disclosing "personal information" to the Ombudsman (or potentially any other complaints handling body) in response to informal or preliminary inquiries. On this analysis, a formal investigation is required before an agency will be satisfied that it is compliant with PPIPA when disclosing personal information to the Ombudsman. This position places both agencies and the Ombudsman conducting a preliminary inquiry in a difficult position.

4.34 The process would be improved if the agency did not have to comply with s 18 of PPIPA (which places limits on the disclosure of

---

58. NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 26.

personal information) as it would be impractical for the agency to obtain the consent of the subject of the inquiry to disclose the information to the Ombudsman. If agencies were required to comply with s 18, then the ability of the Ombudsman to ascertain a complaint's initial merit, or resolve complaints quickly and informally would be encumbered.

4.35 It is this deficiency in s 25 that has led to a direction being made by the Privacy Commissioner entitled "Direction relating to requests made by the Ombudsman under s 13AA of the Ombudsman Act". This direction authorises an agency not to comply with s 16, s 17, s 18, or s 19(1) of PPIPA when the Ombudsman has made a request for information in the course of preliminary inquires pursuant to s 13AA of the *Ombudsman Act 1974* (NSW).

4.36 The Public Interest Advocacy Centre submitted that the *Ombudsman Act 1974* (NSW) should be modified specifically to authorise the Ombudsman to request information for the purpose of preliminary inquiries, with the result that disclosure by an agency would be permitted under s 25 of PPIPA.<sup>59</sup> The *Ombudsman Act 1976* (Cth) has a similar provision.<sup>60</sup>

### The Commission's view

4.37 The most effective way of addressing this issue is by amending the statute regulating the agency. For example, a provision similar to s 7A(1D) of the *Ombudsman Act 1976* (Cth) could be inserted into the *Ombudsman Act 1974* (NSW). That section states:

For the purposes of the *Privacy Act 1988*, the giving of the information to the Ombudsman or the production of the document or record to the Ombudsman is taken to be authorised by law.

4.38 This change will enliven a "required or authorised by or under law" exemption. This suggestion is in line with our recommendations to streamline the exemptions to the Act and to include them in the UPPs where possible.<sup>61</sup> Further, our recommendations in chapter 5 are broad enough to address preliminary inquiries by investigative agencies.<sup>62</sup>

---

59. Public Interest Advocacy Centre, *Submission*, 27.

60. *Ombudsman Act 1976* (Cth) s 7A(1D).

61. See Chapters 4-6.

62. See para 5.33.



**RECOMMENDATION 4.4**

---

Section 13AA of the *Ombudsman Act 1974* (NSW) should be amended to require or authorise the disclosure of personal information by an agency for the purpose of the Ombudsman's preliminary inquiries.



## 5. **Exemptions for law enforcement and investigation**

- Introduction
- General exemptions relating to law enforcement and investigation
- Exemptions for particular agencies

## INTRODUCTION

5.1 Many privacy principles will, at times, be incompatible with law enforcement and investigative agencies' functions and may prejudice operations. Accordingly, it is important that there are adequate exemptions in place to allow law enforcement and investigative agencies to perform their functions without having to comply with privacy principles.

5.2 Privacy legislation allows for this by creating general exemptions relating to law enforcement and investigative agencies, or by specific exemptions for particular bodies.

## GENERAL EXEMPTIONS RELATING TO LAW ENFORCEMENT AND INVESTIGATION

### Legislative provisions

5.3 Sections 23 and 24 of the *Privacy and Personal Information Protection Act 1998* (NSW) ("PPIPA") provide exemptions to law enforcement and investigative agencies. Section 23 exempts particular agencies from compliance with the Information Protection Principles ("IPPs") that would serve to impede or prejudice law enforcement functions. PPIPA identifies particular agencies as law enforcement agencies.<sup>1</sup> However, most provisions of s 23 also apply to any public sector agency.<sup>2</sup> A law enforcement agency or public sector agency will not be required to comply with s 9, s 10, s 17, s 18 and s 19 of PPIPA in the prescribed circumstances.

- 
1. *Privacy and Personal Information Protection Act 1998* (NSW) s3. A "law enforcement agency" means any of the following: (a) the NSW Police Force, or the police force of another State or a Territory; (b) the NSW Crime Commission; (c) the Australian Federal Police; (d) the Australian Crime Commission; (e) the Director of Public Prosecutions of NSW, of another State or a Territory, or of the Commonwealth; (f) the Department of Corrective Services; (g) the Department of Juvenile Justice; or (h) a person or body prescribed by the regulations for the purposes of this definition.
  2. *Privacy and Personal Information Protection Act 1998* (NSW) s 23, other than s 23(1).

5.4 Section 24 exempts investigative agencies<sup>3</sup> from compliance with s 9, s 10, s 12(a), s 17 and s 18 of PPIPA. An investigative agency need not comply with s 9 and s 10 if compliance would detrimentally affect the agency's complaint handling or investigative functions. The investigative agency need not comply with s 17 if non-compliance is reasonably necessary to exercise the agency's complaint or investigative functions. Further, an investigative agency is permitted not to comply with s 18 if the information is disclosed to another investigative body. The exemptions under s 24 also extend to agencies investigating or handling a complaint in circumstances where referral could be made to or from an investigative agency.<sup>4</sup>

5.5 Under the *Health Records and Information Privacy Act 2002* (NSW) ("HRIPA"), the exemptions provided to law enforcement and investigative bodies are contained within the relevant Health Privacy Principles ("HPPs").<sup>5</sup> Significantly, the wording of the law enforcement exemptions under HRIPA, which differ from s 23 of PPIPA, provide a uniform and more clearly focused test. The law enforcement exemptions under HRIPA are restricted to circumstances where there are reasonable grounds to believe that an offence has been, or will be committed. It was on this basis that both Privacy NSW and the Statutory Review of PPIPA recommended that s 23 replicate the HRIPA provisions.<sup>6</sup>

5.6 Similarly in regard to investigative agencies, HRIPA provides a different, and arguably simpler, test by focusing on the exercise of

- 
3. Defined in *Privacy and Personal Information Protection Act 1998* (NSW) s 3 and *Health Records and Information Privacy Act 2002* (NSW) s 4 to mean any of the following: the Ombudsman's Office; the Independent Commission Against Corruption; the Inspector of the Independent Commission Against Corruption; the Police Integrity Commission; the Inspector of the Police Integrity Commission and any staff of the Inspector; the Health Care Complaints Commission; the Office of the Legal Services Commissioner; or a person or body prescribed by the regulations for the purpose of this definition.
  4. *Privacy and Personal Information Protection Act 1998* (NSW) s 24.
  5. For law enforcement agencies see *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPPs 4(4)(e), 10(1)(g), 10(1)(i), 11(1)(h), 11(1)(j); for investigative agencies see sch 1 HPPs 4(4)(f), 4(7), 5(3), 10(1)(h)(ii), 10(1)(j), 10(3), 10(5), 11(1)(k), 11(2)(c), 11(3), 11(6).
  6. NSW Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly) ("Statutory Review of PPIPA") Recommendation 19; Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 51, 85.

complaint handling functions or investigative functions of investigative agencies.<sup>7</sup>

### Issues raised by s 23 of PPIPA

5.7 The following issues have been raised with regard to s 23:

- (1) The number of different tests included in s 23 makes interpretation difficult. As Privacy NSW have commented, s 23 uses nine different tests for non-compliance with the IPPs.<sup>8</sup>
- (2) The absence of definitions causes a difficulty in application. The NSW Government has acknowledged that this “lack of clarity means that agencies are unclear about whether they can share otherwise protected personal information”.<sup>9</sup> Concern has been raised that failure to define the terms “law enforcement functions” and “law enforcement purposes”<sup>10</sup> may lead to agencies interpreting them to cover “every context where an agency is seeking to give effect to its legal powers and responsibilities”.<sup>11</sup> Such an interpretation would defeat the underlying purpose of the Act. It has been submitted that, properly construed, the term “law enforcement” should be limited to “expediting the investigation of matters that involve breaches of the criminal

---

7. *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPPs 10(1)(j) and 11(1)(k); noting also the exemption is extended to any public sector agency, or public sector official, 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: sch 1 HPPs 10(5) and 11(6).

8. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 84.

9. NSW Government, *Response to the Report on the Statutory Review of the Privacy and Personal Information Protection Act 1998* (“NSW Government Response to the Statutory Review”) 9.

10. “Law enforcement purposes” is also used in cl 2 of NSW Privacy Commissioner, “Direction On Information Transfers Between Public Sector Agencies”, Public Interest Direction (21 December 2009).

11. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 84.

law and the preparation of cases before courts or tribunals”.<sup>12</sup> The Administrative Decisions Tribunal (“ADT”) has supported this view, limiting the application of s 23 to criminal law enforcement.<sup>13</sup>

- (3) Some agencies engaged in non-criminal law enforcement are concerned that they do not get the benefit of the exemption because the exemption is limited to criminal law enforcement. This may hamper some agencies’ ability to function effectively. NSW Fair Trading submitted that the definitions of law enforcement and investigative agencies “are narrowly formulated and do not take account of the functions of an agency like the Office of Fair Trading”.<sup>14</sup> On this analysis, the exemption would not apply to disciplinary or professional conduct inquiries and investigations;<sup>15</sup> agencies investigating licensing or business transactions; or enforcement of civil law.<sup>16</sup>
- (4) There is confusion surrounding the phrase “for the protection of public revenue” contained in s 23.<sup>17</sup> In its submission to the Statutory Review of PPIPA, Privacy NSW queried whether this exemption was “aimed at the pursuit of monies owing to the State such as unpaid fines, and/or to prevent fraud against consolidated revenue, and/or to prevent waste or misuse of public money”.<sup>18</sup> The Privacy Commissioner has suggested that this broader interpretation should not apply, and that

---

12. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 85.

13. See *BY v Director General, Attorney General’s Department (No. 2)* [2003] NSWADT 37, [43]-[53] and cases discussed therein; *JD v Department of Health (GD)* [2005] NSWADTAP 44, [98]-[107]; *JD v NSW Medical Board* [2005] NSWADT 247, [40].

14. NSW Office of Fair Trading, *Submission*, 2.

15. See *JD v Department of Health* [2005] NSWADTAP 44, [98]-[107].

16. NSW Office of Fair Trading, *Submission*, 2.

17. A public sector agency (whether or not a law enforcement agency) is not required to comply with s 17 or s 18 if reasonably necessary for the protection of the public revenue: *Privacy and Personal Information Protection Act 1998* (NSW) s 23(4), s 23(5).

18. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 85.

merely saving money is not supported by the term “revenue”. The application of the provision to “collection of income in the form of fines”, or government charges for services is also unclear.<sup>19</sup>

### Issues raised by s 24 of PPIPA

5.8 A number of issues have arisen in respect of s 24. These include:

- (1) the broad formulation of s 24;
- (2) the inability of agencies generally to disclose to investigative agencies;
- (3) section 24’s inapplicability to agencies without coercive powers;
- (4) the lack of provision for preliminary inquiries; and
- (5) the failure to deal with sensitive information.

#### *Broad formulation of the provision*

5.9 Questions have been raised about the level of exemption from the IPPs, with the suggestion that the exemption should be more restricted and contained within the relevant IPP.<sup>20</sup> This is the approach adopted in HRIPA and the *Privacy Act 1988* (Cth).

#### *Inability of agencies generally to disclose to investigative agencies*

5.10 The exemptions do not 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, *unless* the agency is itself investigating a complaint 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”.<sup>21</sup>

---

19. Privacy NSW, *A Guide to the Information Protection Principles* (1999) 34.

20. Cyberspace Law and Policy Review Centre, *Submission*, 28; Australian Privacy Foundation, *Submission*, 11.

21. *Privacy and Personal Information Protection Act 1998* (NSW) s 24(4).



5.11 The Statutory Review of PPIPA recommended adopting “investigative agencies” provisions similar to those found in HRIPA.<sup>22</sup> For example, the wording under HPP 11(1)(k) (which deals with the disclosure of health information) provides an exemption to disclosure where:

the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies.<sup>23</sup>

5.12 HRIPA therefore contemplates, more generally, disclosure to investigative agencies. In comparison, PPIPA continues to rely on public interest directions (“PIDs”) made by the Privacy Commissioner pursuant to s 41 of PPIPA to address this issue. The PID entitled “Direction on Processing of Personal Information by Public Sector Agencies in Relation to their Investigative Functions” attempts to fill this gap. It permits non-compliance with all IPPs (except s 11, s 12 and s 16) where non-compliance is reasonably necessary for the proper exercise of an agency’s investigative functions or in the course of a lawful investigation,<sup>24</sup> and permits agencies to disclose personal information to other agencies where it is reasonably necessary to assist another agency exercising investigative functions or conducting a lawful investigation.<sup>25</sup>

*Inapplicability to agencies without coercive powers*

5.13 Section 24 does not apply to situations where an agency without coercive powers conducts an investigation. Privacy NSW has flagged this issue, recognising that there may be an investigation by or within a public sector agency that may require non-compliance with an IPP. This may include investigations of staff misconduct or disciplinary matters, or investigations of parties to determine whether a breach of a condition or

---

22. Statutory Review of PPIPA, Recommendation 19.

23. A secondary purpose is a purpose other than the purpose for which it was collected.

24. NSW Privacy Commissioner, “Direction on Processing of Personal Information by Public Sector Agencies in Relation to their Investigative Functions”, Public Interest Direction (21 December 2009) cl 4.

25. NSW Privacy Commissioner, “Direction on Processing of Personal Information by Public Sector Agencies in Relation to their Investigative Functions”, Public Interest Direction (21 December 2009) cl 4A.

licence has occurred (such as a breach of a tenancy agreement or pollution laws).<sup>26</sup>

5.14 As a response to this, Privacy NSW submitted that:

consideration be given to the incorporation of a more comprehensive exemption for investigations conducted by or within general public sector agencies, so as to obviate the need for future public interest directions or code provisions.<sup>27</sup>

5.15 HRIPA addresses these issues in the HPPs, allowing for disclosure to investigative agencies generally when reasonably necessary for the exercise of complaint handling functions or investigative functions.<sup>28</sup> HPPs 10(5) and 11(6) extend this exemption from use and disclosure HPPs to:

any public sector agency, or public sector official, 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.<sup>29</sup>

5.16 There is also a provision under the HPPs that provides exemptions when an agency suspects unlawful activity, unsatisfactory professional conduct or conduct that may be grounds for disciplinary action.<sup>30</sup> This, arguably, includes the internal disciplinary investigations of agencies.<sup>31</sup>

5.17 The PID entitled “Direction on Processing of Personal Information by Public Sector Agencies in Relation to their Investigative Functions” attempts to deal with this issue under PPIPA. Relevantly, this contains two clauses providing exemptions. Clause 4 exempts compliance from s 9, s 10, s 13, s 14, s 15, s 17, s 18 and s 19 of PPIPA if non-compliance is reasonably necessary for the proper exercise of any of the agency’s

---

26. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 86-87.

27. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 87.

28. *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPP 11(1)(k).

29. This, however, does not apply to certain bodies with investigative functions, for example, the NSW Office of Fair Trading. This could be overcome by amending the definition of investigative agency: see Recommendation 5.1.

30. *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPP 11(1)(i).

31. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 87.

investigative functions or its conduct of any lawful investigations.<sup>32</sup> Clause 4A was inserted in order to ensure that disclosure between agencies for the purpose of assisting an agency to perform investigative functions is permitted.<sup>33</sup>

5.18 Privacy codes have also been created to fill the gap. The majority of codes have provisions exempting the investigative and complaint-handling functions of agencies from various IPPs.<sup>34</sup> An example is the Privacy Code for NSW Fair Trading. It exempts NSW Fair Trading from all the IPPs except s 8, s 11, s 12 and s 16 where compliance is “reasonably likely to detrimentally affect (or prevent the proper exercise of) investigative or law enforcement activities”.<sup>35</sup>

*Lack of provision for preliminary inquiries*

5.19 The “Direction on Processing of Personal Information by Public Sector Agencies in Relation to their Investigative Functions”, while broadening the exemption for investigative agencies, covers only those investigations which may lead to formal action, not preliminary or informal inquiries unless directly related to lawful investigation.<sup>36</sup> HPPs 10(1)(j), 10(5), 11(1)(k) and 11(6) of HRIPA are broadly worded and may facilitate preliminary inquiries. Under PPIPA, no provision is made for preliminary inquiries, which are addressed in chapter 4.<sup>37</sup>

---

32. For the interpretation of this clause see: *NW v NSW Fire Brigades* [2005] NSWADT 73. See also *Commissioner of Police, New South Wales Police Force v YK (GD)* [2008] NSWADTAP 78.

33. This provides that “[a] relevant agency need not comply with sections 18 or 19(1) of the PPIP Act if non-compliance is reasonably necessary to assist another relevant agency exercising investigative functions or conducting a lawful investigation”.

34. *Privacy and Personal Information Protection Act 1998* (NSW) s 24(4).

35. See *Privacy Code of Practice for the NSW Department of Fair Trading*, Principles 2, 6-8, 10, 13-15.

36. NSW Privacy Commissioner, “Direction on Processing of Personal Information by Public Sector Agencies in Relation to their Investigative Functions”, Public Interest Direction (21 December 2009) cl 4, cl 4A.

37. See para 4.32-4.38.

*Failure to deal with sensitive information*

5.20 Section 19(1) of PPIPA prevents disclosure of sensitive information<sup>38</sup> and it is not exempted under s 24.<sup>39</sup> The “Direction on Processing of Personal Information by Public Sector Agencies in Relation to their Investigative Functions” gives an exemption from s 19(1) to agencies disclosing personal information to assist another relevant agency exercising investigative functions or conducting a lawful investigation. It is obvious that exemption from this IPP will on occasion be necessary to assist an investigation.

**Law enforcement and investigation under the UPPs**

5.21 This section addresses the relationship between the proposed Unified Privacy Principles (“UPPs”) and law enforcement and investigative exemptions contained in NSW privacy legislation. It also considers whether the exemptions under the UPPs are appropriate for NSW in light of the issues raised in respect of PPIPA s 23 and s 24.<sup>40</sup>

5.22 Law enforcement and investigative agencies are treated together under the UPPs. The UPPs use the phrase “enforcement body”, which is defined to include both law enforcement and investigative bodies.<sup>41</sup> Adopting the UPPs in NSW would require that the definition of “enforcement body” in PPIPA include all the bodies currently listed as either a “law enforcement agency” or an “investigative agency” in s 3 of PPIPA. The definition of “enforcement body” under the *Privacy Act 1988* (Cth) goes further than PPIPA and HRIPA in that it includes “a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction

---

38. This term is not used in the *Privacy and Personal Information Protection Act 1998* (NSW), but covers similar types of information for which the term is used under the UPPs.

39. *Privacy and Personal Information Protection Act 1998* (NSW) s 23 acknowledges that this may be necessary; s 23(7) provides: “A public sector agency (whether or not a law enforcement agency) is not required to comply with section 19 if the disclosure of the information concerned is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed”.

40. See para 5.7-5.20.

41. “Enforcement body” is defined in *Privacy Act 1988* (Cth) s 6.

or a prescribed law”.<sup>42</sup> In order to address the concerns of some stakeholders,<sup>43</sup> this should be included in the definition of “enforcement body” under PPIPA.

5.23 The UPPs provide exemptions for law enforcement and investigative functions in four main ways:

- (1) ***Where non-compliance is necessary for a relevant function of an enforcement body.*** UPP 5.1(f) lists a number of circumstances where non-compliance with UPP 5 (Use and Disclosure) is necessary for “an enforcement body”.
- (2) ***Where non-compliance is reasonable, or compliance is impracticable.*** Terms such as “reasonable” or “practicable” – including their antonyms “unreasonable” or “impracticable” – are intended to allow for a range of circumstances in which non-compliance would be appropriate.<sup>44</sup> Law enforcement and investigative agencies would be able to rely on these terms to avoid having to comply with particular UPPs in certain circumstances. Determining “reasonableness” involves making an evaluative judgement.<sup>45</sup> The standard of what is reasonable and practicable would obviously depend on the circumstances of each case together with the function and

---

42. *Privacy Act 1988* (Cth) s 6; there is a similar definition in the *Information Privacy Act 2000* (Vic) s 3 “law enforcement agency”.

43. For example, the NSW Office of Fair Trading, see para 5.7, 5.18.

44. Law enforcement and investigative agencies may be able to rely on these terms in UPPs 1, 2.2, 2.3, 2.4, 3 and 7 to avoid compliance with a UPP. For example, UPP 2.3 provides that “if it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual”. There will be circumstances in the course of law enforcement where it will not be reasonable or practicable to comply with this privacy principle. In such instances, non-compliance will be permitted on the wording of this provision. It is apparent that this provision is intended to preserve law enforcement functions and maintain an exemption where compliance with the UPPs would prejudice the purpose of collection: see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”), vol 1, [21.32].

45. NSW Law Reform Commission, *Privacy Principles*, Report 123 (2009) (“NSWLRC Report 123”) [2.43].

aims of the agency.<sup>46</sup> The application of these principles will be aided by guidelines and codes issued by the Privacy Commissioner.

- (3) *Where non-compliance is required or authorised under law.* Law enforcement and investigative agencies would also be able to claim exemptions under the “required or authorised by or under law” exception to certain UPPs.<sup>47</sup> UPPs 2.5(b), 5.1(c), 8.1(b) and 11.1 provide that non-compliance with the relevant UPP will be permitted when “required or authorised by or under law”. If a law enforcement or investigative agency has the appropriate legal backing to require or authorise either its, or another agency’s non-compliance, then this will be sufficient to avoid compliance with a relevant privacy principle under the above-mentioned UPPs.<sup>48</sup> The meaning of “required or authorised by or under law” is discussed in chapter 4.
- (4) *Where necessary to lessen or prevent a serious threat.* UPP 5.1(c) indicates that compliance is not required where the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to: (i) an individual’s life, health or safety; or (ii) public health or public safety. This provides an additional general exception which may be relied on by agencies (whether or not

---

46. The Commission recommends that “[t]he legislation containing the UPPs should provide that, subject to express contrary intention, where a matter in the UPPs is described, characterised or referred to as reasonable or unreasonable, or is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner, the standard to be applied in determining whether the matter is reasonable or unreasonable, or has been carried out or otherwise dealt with reasonably or in a reasonable manner, is what a reasonable person would consider appropriate in the circumstances”: NSWLRC Report 123, Recommendation 2.

47. A similar exemption is already provided in *Privacy and Personal Information Protection Act 1998* (NSW) s 25. However, if the UPPs are adopted in NSW, *Privacy and Personal Information Protection Act 1998* (NSW) s 25 should be repealed: see Recommendation 4.1.

48. If an enforcement agency has a legal obligation or right to require, use or disclose information, then the UPPs are not intended to interfere with this: see, eg, ALRC Report 108, vol 2 [25.99].

“enforcement bodies”) in circumstances obviously requiring use or disclosure, but where none of the other exceptions are applicable, or where applicability may be more difficult to demonstrate.

5.24 We now discuss these exemptions in relation to the relevant privacy principles addressed in s 23 and s 24 of PPIPA. We examine the extent to which the proposed UPPs regulate privacy principles akin to those principles listed in s 23 and s 24. The above exemptions operate to exempt law enforcement and investigative agencies, in certain circumstances, from compliance with privacy principles relating to Collection (UPP 2), Notification (UPP 3), Data Security (UPP 8), Use and Disclosure (UPP 5) and Access and Correction (UPP 9).

### *Collection*

5.25 UPP 2.3 provides that “if it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual”. Often in the course of law enforcement or an investigation it will not be reasonable or practicable to comply with this privacy principle. In its response to the UPPs, the Commonwealth Government agreed that “there will be many situations, particularly for agencies, where it will not be reasonable or practicable to collect personal information directly from the individual concerned”.<sup>49</sup> In such instances, non-compliance will be permitted on the wording of this provision. This would cover s 23(1) and s 23(2) of PPIPA in relation to law enforcement agencies, and s 24(1) and s 24(6) in relation to investigative agencies.

5.26 The UPPs, however, would not entirely cover s 24(6) of PPIPA, which grants the Ombudsman’s Office complete exemption from s 9 and s 10. Under the UPPs, the Ombudsman’s Office would get similar exemptions to other investigative bodies if included in the definition of “enforcement body”. The exemptions from s 9 and s 10 are both covered by the “reasonableness” provisions in the UPPs and so further exemption seems unnecessary.

5.27 Further, the reasonableness provisions in the collection and notification UPPs (2.3(b) and 3) would allow NSW Fair Trading to

---

49. Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice* (2009) 40.

operate effectively as an agency with law enforcement and investigative functions. This is currently being achieved through privacy codes of practice.<sup>50</sup>

5.28 We note that UPP 2.5 prohibits the collection of sensitive information unless one of the exceptions is satisfied.<sup>51</sup> This is significant for law enforcement and investigative agencies whose functions will often require the collection of such information. The Australian Government responded to this by expanding the listed exceptions to the collection of sensitive information to include the investigation of various matters in circumstances aligned with the National Privacy Principles (“NPPs”) 2.1(f)<sup>52</sup> and (h).<sup>53</sup>

### *Notification*

5.29 It is of particular importance that, in respect of a law enforcement or investigative agency’s law enforcement or investigative functions, there is no requirement for the investigative agency to comply with the notification principle (UPP 3). In the course of law enforcement or an investigation, compliance with this principle could prejudice an operation

---

50. See para 5.18.

51. This includes where the collection is required or authorised by law and where the collection is necessary to prevent or lessen a serious threat to the life or health of any individual. See also Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice* (October 2009) 43-44.

52. “[T]he organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities”.

53. “[T]he organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body: (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; (iii) the protection of the public revenue; (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.”: See Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice* (2009) 43.



if the individual was put on notice. The notification principle only applies where “reasonable in the circumstances”. Accordingly, no steps need to be taken by the investigative agency if it would not be “reasonable in the circumstances”. As the Australian Law Reform Commission (“ALRC”) has pointed out:

It is clearly not reasonable to notify an individual of the fact of collection when a law enforcement agency is collecting intelligence on a person who is suspected of committing an offence, or where to do so would identify an informant during the investigative process.<sup>54</sup>

5.30 The proposed UPPs would, therefore, cover s 23(3) and s 24(1) of PPIPA, which provide an exemption to similar notification requirements.

#### *Data security*

5.31 Sub-section 24(7) of PPIPA provides that an investigative agency is not required to comply with s 12(a), which deals with the retention of personal information.<sup>55</sup> Under the UPPs, this exemption would be covered by the wording of UPP 8 (Data Security). UPP 8 does not go as far as s 24(7) in completely exempting compliance. It qualifies compliance with the principle by requiring that an agency take reasonable steps to “destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs”. If an investigative agency still has a use for the personal information, or has good grounds for believing that the kind of information would be of assistance,<sup>56</sup> then the investigative agency may retain the personal information. UPP 8 has the benefit that where an agency no longer has a use for personal information, it must comply with the principle. Section 24(7) does not provide a similar qualification. Despite this narrowing of scope, s 24(7) of PPIPA is, to the extent necessary, covered by UPP 8.

#### *Use and disclosure*

5.32 UPP 5.1 provides a number of circumstances permitting non-compliance with the use and disclosure principle which are relevant for enforcement bodies. This includes where the use or disclosure is necessary to prevent a serious threat (UPP 5.1(c));<sup>57</sup> required or authorised

---

54. ALRC Report 108, vol 2, [37.111].

55. See *Health Records and Information Privacy Act 2002* (NSW) s 5(3).

56. ALRC Report 108, vol 2, [37.112].

57. See para 5.23.

by or under law (UPP 5.1(e));<sup>58</sup> where there is suspicion of unlawful activity or serious misconduct (UPP 5.1(d)); or where necessary for an enforcement body (UPP 5.1(f)). UPP 5.1(f) provides an exception to the use and disclosure principle where the agency or organisation reasonably believes that the use or disclosure is necessary for one or more of the following by, or on behalf of, an enforcement body:

- (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
- (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
- (iii) the protection of the public revenue;
- (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
- (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal;

5.33 UPP 5.1(f) is obviously similar to s 23(4), (5), (7) and s 24(2), (3), (4) of PPIPA which allow agencies and law enforcement and investigative agencies to avoid the use and disclosure principles in certain circumstances.<sup>59</sup> However, the test under UPP 5.1(f) is broader and more flexible, allowing an enforcement body or agency to use or disclose personal information if necessary in the prescribed circumstances. Depending on the circumstances, this may include preliminary inquiries.

5.34 Clause 4A of the “Direction on Processing of Personal Information by Public Sector Agencies in Relation to their Investigative Functions” was inserted to make it clear that an agency could disclose personal information to another agency with respect to that other agency’s investigative functions. The wording of UPP 5.1(f) is similar and has the same effect.<sup>60</sup>

---

58. See para 5.23 and Chapter 4.

59. See also *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPPs 10(1)(f) and 11(1)(j).

60. An issue raised was that there should be an onus on the “agency disclosing the information to demonstrate that the information was related to an investigation of a possible offence”: NSW FOI/Privacy Practitioners’ Network, *Submission*, 10.

5.35 Further, this provision has the benefit that the types of law enforcement functions are set out. The ambiguity inherent in s 23 as to what constitutes a law enforcement function is largely resolved in that the exemption applies to “the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law”. This is sufficiently broad to remedy the concerns of some agencies<sup>61</sup> that they may not get the benefit of the exemption because they do not have a criminal law enforcement function and thus require a code to gain exemption. Under the UPPs, they would gain the benefit of the exemption, provided they satisfied the requirements of UPP 5.1(f).

5.36 The UPPs sufficiently cover the PID in relation to agencies conducting their own investigations.<sup>62</sup> Proposed UPP 5.1(d), as modified by us,<sup>63</sup> states that personal information can be used or disclosed if:

the agency or organisation has reason to suspect that unlawful activity or serious misconduct relating to its operations has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

5.37 The requirement that the serious misconduct relates to the operations of the agency covers all relevant situations requiring an internal investigation.<sup>64</sup> An agency should not be required to disclose personal information to another agency relating to an individual where the misconduct relates only to the operations of the second agency. If the misconduct is serious and widespread enough that it involves both agencies, then the matter should perhaps be referred to the Ombudsman or another independent agency for investigation. This is implied by Note 2 to UPP 5 which states that:

---

In practice this may require a written request by the investigative agency detailing the necessity of disclosure in relation to an investigation or complaint. This is a requirement under UPP 5.2.

61. For example, the NSW Office of Fair Trading, *Submission*, 2.

62. For further analysis see NSWLRC Report 123, Chapter 5, specifically Recommendation 6 and the preceding paragraphs.

63. NSWLRC Report 123, Recommendation 6.

64. Note that the requirement of “relating to its [the agency’s] operations” applies only to serious misconduct and not to unlawful activity.

Nothing in subclause 5.1 requires an agency or organisation to disclose personal information; an agency or organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

5.38 UPP 5.1 strikes an appropriate balance between the need of agencies to use and disclose information for the purposes of certain investigations and the protection of individual privacy. It will not allow an exception to collection or disclosure principles in the resolution of a frivolous or non-serious complaint or for the investigation of a minor disciplinary matter.

5.39 There is no additional requirement for the use or disclosure of sensitive information under the UPPs. This type of information may be used or disclosed in accordance with the normal exceptions to use and disclosure. However, because sensitive information warrants a higher degree of protection than other information, the Privacy Commissioner may wish to issue guidelines in this regard.

#### *Access and correction*

5.40 UPP 9 provides that an agency must provide an individual with access to personal information held by the agency and to amend the information when requested by the individual. UPP 9 is subject to other laws<sup>65</sup> and consequently if access is denied under the *Freedom of Information Act 1989* (NSW) (“FOI Act”), access would be denied under privacy legislation. This approach is supported by the Commonwealth Government in its response to the proposed UPPs.<sup>66</sup>

5.41 Sections 23 and 24 of PPIPA do not provide an exemption to the equivalent access and correction principles under that Act.<sup>67</sup> The exemptions to these principles are instead to be found in the FOI Act<sup>68</sup> and we note that the *Government Information (Public Access) Act 2009*

---

65. UPP 9.1(a).

66. Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice* (2009) 64.

67. *Privacy and Personal Information Protection Act 1998* (NSW) s 13, s 14, s 15; see also *Health Records and Information Privacy Act 2002* (NSW) s 29, sch 1 HPPs 6, 7, 8.

68. *Privacy and Personal Information Protection Act 1998* (NSW) s 5, s 20(5), s 25; see also discussion in NSWLRC Report 123, [9.58]-[9.64] and [9.117]-[9.120].

(NSW) has amended these exemptions to access to personal information.<sup>69</sup> This is similar to the approach taken under HRIPA.<sup>70</sup>

5.42 Under both of these approaches, an enforcement body would gain exemption by way of laws external to PPIPA, mainly by virtue of the FOI Act.

### The Commission's view

5.43 We are satisfied that the UPPs are broad and flexible enough to cover the exemptions contained in s 23 and s 24 of PPIPA, and are sufficiently flexible to remedy some of the defects in s 23 and s 24 that the codes and s 41 PIDs have sought to address. We believe that the exceptions contained in the UPPs also improve upon s 23 and s 24 in that they are not overly prescriptive and contemplate a wide range of circumstances. There is nothing in s 23 or s 24 that requires additional changes to the UPPs; with the exception of the NSW Police Force,<sup>71</sup> law enforcement and investigative agencies will, to a large extent, be subject to the same rules and principles as they were previously under s 23 and s 24. Consequently, in the event that the UPPs are adopted in NSW, we recommend the repeal of s 23 and s 24 of PPIPA.

5.44 The definition of “enforcement body” as used in the UPPs would need to include the current “law enforcement agencies” and “investigative agencies” listed in s 3 of PPIPA.<sup>72</sup> Further, in order to ensure that the concerns of NSW Fair Trading are accommodated, the definition of “enforcement body” under the UPPs will need to include a provision mirroring that of the *Privacy Act 1988* (Cth), which includes “a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law”.<sup>73</sup> This will extend the current scope of s 23 beyond criminal law.

---

69. See NSW Law Reform Commission, *Access to Personal Information*, Report 126 (2010) (“NSWLRC Report 126”) Chapter 3 generally.

70. *Health Records and Information Privacy Act 2002* (NSW) s 22(3); see also HPPs 6(2)(a), 7(2)(a), 8(4)(a).

71. See Recommendation 5.4 and para 5.60, 5.64-5.65.

72. NSWLRC Report 123, [5.76].

73. *Privacy Act 1988* (Cth) s 6; there is a similar definition in the *Information Privacy Act 2000* (Vic) s 3 “law enforcement agency”.

## RECOMMENDATION 5.1

---

If the UPPs are adopted in NSW:

- (1) s 23 and s 24 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed;
- (2) the definition of “enforcement body” should include the “law enforcement agencies” and “investigative agencies” listed in s 3 of the *Privacy and Personal Information Protection Act 1998* (NSW); and
- (3) the definition of “enforcement body” should include an authority to the extent that it is responsible for administering, or performing a function under:
  - (a) a law that imposes a penalty or sanction; or
  - (b) a prescribed law.

### *Law enforcement agencies*

5.45 In the event that the UPPs are not adopted, we recommend that s 23 should be amended to replicate the equivalent exemptions under HRIPA.<sup>74</sup> For example, where the use or disclosure is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed.<sup>75</sup> This would produce a clearer and more practical test for agencies relying on an exemption in relation to law enforcement functions.

5.46 If the UPPs are not adopted in NSW, it is further recommended that the definition of “law enforcement agency” in s 3 of PPIPA be amended to include an authority to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law. This is for the reasons outlined above.<sup>76</sup>

---

74. See HPPs 4(4)(e), 10(1)(g), 10(1)(i), 11(1)(h), 11(1)(j).

75. *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPPs 10(1)(i) and 11(1)(j).

76. See para 5.7, 5.22, 5.44.

5.47 The meaning of “law enforcement functions” and “for the protection of public revenue” should be left to guidelines issued by the Privacy Commissioner.

## RECOMMENDATION 5.2

If the UPPs are not adopted in NSW:

- (1) s 23 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to replicate the wording of the equivalent exemptions under the *Health Records and Information Protection Act 2002* (NSW); and
- (2) the definition of “law enforcement agency” should include an authority to the extent that it is responsible for administering, or performing a function under:
  - (a) a law that imposes a penalty or sanction; or
  - (b) a prescribed law.

### *Investigative agencies*

5.48 Investigative agencies play a fundamental role in ensuring that public sector agencies are acting responsibly in accordance with their functions, and according to law. There are therefore good policy reasons to justify provisions in PPIPA that facilitate, rather than impede, this purpose. Most submissions accepted this broad proposition, but differed as to how it would best be implemented.

5.49 We recommend that the approach taken in HRIPA be replicated in PPIPA. Under HRIPA the use or disclosure of the information for the secondary purpose (a purpose other than the purpose for which it was collected) must be reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies.<sup>77</sup> This should apply to both use and disclosure principles. This is a flexible approach and has the benefit of being of general application, avoiding the need for a PID or privacy code.

77. *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPPs 10(1)(j) and 11(1)(k).

5.50 Further, under HPP 11(6),<sup>78</sup> exemptions apply to an agency or official 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. This will facilitate agencies conducting their own disciplinary investigations.

5.51 Sub-sections 24(2), (3) and (4) of PPIPA should be amended to exempt agencies from s 18 and s 19(1) of PPIPA when disclosing information to an investigative agency for the purpose of that investigative agency carrying out its complaints-handling or investigative functions. This is to ensure that sensitive information may be disclosed in certain circumstances.

5.52 Disclosure to agencies for the purposes of preliminary investigations would be covered by amending s 24 to imitate the approach under HPPs 10(1)(j), 10(5), 11(1)(k) and 11(6) of HRIPA which are worded broadly enough to address this issue.<sup>79</sup> Further, we recommend elsewhere in this report that s 25 of PPIPA be amended to contain a single “required or authorised by or under law” exemption.<sup>80</sup> Any concerns in relation to an agency’s ability to authorise the disclosure of personal information during preliminary inquiries would be addressed by including a provision similar to HPPs 10(5) and 11(6) as well as our recommendations in respect of s 25.<sup>81</sup>

5.53 Finally we are of the view that the Ombudsman’s Office is already suitably protected under PPIPA so as to require no further exemption under s 24(6). As an “investigative agency”, the Ombudsman’s Office already has the necessary scope for non-compliance with s 9 and 10 of PPIPA under s 24(1).<sup>82</sup>

---

78. “The exemptions provided by subclauses (1)(k) and (2) extend to any public sector agency, or public sector official, 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”; see also HPP 10(5).

79. The use or disclosure only needs to be reasonably necessary for the exercise of complaint handling or investigative functions.

80. See Recommendations 4.1-4.3.

81. See Chapter 4.

82. See Chapter 4. See particularly Recommendation 4.4.



### RECOMMENDATION 5.3

---

If the UPPs are not adopted in NSW:

- (1) s 24 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to mirror the wording of the equivalent provisions in the HPPs; and
- (2) s 24(6) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

## EXEMPTIONS FOR PARTICULAR AGENCIES

5.54 Section 27 of PPIPA and s 17 of HRIPA specifically exempt the Independent Commission Against Corruption, the NSW Police Force, the Police Integrity Commission and the NSW Crime Commission from compliance with all of the IPPs,<sup>83</sup> and compliance with the Act as a whole for HRIPA, unless the information is in connection with the exercise of their “administrative and educative functions”.<sup>84</sup>

### Administrative and educative functions

5.55 Administrative functions include “corporate services areas performing functions such as personnel, budget and information technology”.<sup>85</sup> Educative functions include community, school and internal training programs.<sup>86</sup> The meanings of these terms, however, are not settled and may be construed more narrowly than Parliament intended. The then Attorney General, the Hon JW Shaw, explained the purpose of s 27 as follows:

The purpose of the legislation is not to protect secrecy in dealings or to protect the Government from accountability for its actions, and accordingly there are generous exemptions in the bill for such investigative agencies as the Independent Commission Against Corruption, the Police Integrity Commission and the New South Wales Crime Commission, which have to comply with the

---

83. *Privacy and Personal Information Protection Act 1998* (NSW) s 27(1).

84. *Privacy and Personal Information Protection Act 1998* (NSW) s 27(2).

85. *HW v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 214, [30].

86. *HW v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 214, [31].

information protection principles in connection with the exercise of their administrative and educative functions. A similar exemption is provided for the Police Service.<sup>87</sup>

5.56 Privacy NSW has interpreted this to mean that the purpose of s 27 is to “ensure accountability of the Government”.<sup>88</sup> The concern is that the terms “administrative and educative functions” are being interpreted narrowly so as to leave few activities or functions of the bodies listed in s 27 subject to the privacy principles.

5.57 The difficulty faced in distinguishing administrative functions from operational functions is illustrated in *YK v Commissioner of Police, NSW Police*.<sup>89</sup> 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.

5.58 On appeal, the Appeal Panel of the ADT decided that the correct approach to the interpretation of s 27 is to view it as providing “a blanket exclusion from the application of the Act to the named agencies in respect of all their activities” subject to the qualification of “administrative and educative functions”. Consequently, if the impugned conduct is either administrative or educative, then it is “brought back under the regulation of the Act”. The corollary is that any conduct or function not “administrative” or “educative” is wholly exempt from the IPPs.<sup>90</sup>

---

87. New South Wales, *Parliamentary Debates*, Legislative Council, Second Reading Speech, 17 September 1998, 7599.

88. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 72.

89. *YK v Commissioner of Police, New South Wales Police* [2008] NSWADT 81.

90. *Commissioner of Police, New South Wales Police Force v YK (GD)* [2008] NSWADTAP 78, [20].

5.59 On this basis, conduct involving mixed functions is exempt.<sup>91</sup> This categorisation by default broadens the scope of s 27 of PPIPA and s 17 of HRIPA.

5.60 Some stakeholders have argued that the exemption is miscast in that only legitimate operational functions ought to be exempt.<sup>92</sup> It may be more appropriate to grant an exemption from certain IPPs,<sup>93</sup> so that some IPPs are applicable, for example: data quality, security and retention.<sup>94</sup> Particular concern was expressed about the implication of the NSW Police Force's exemption from IPPs. It was argued that the data quality principle should be applied to criminal records, given the repercussions of inaccurate data.<sup>95</sup> For example, s 27 has been used to exempt the Police from compliance with privacy principles in cases where the Police mixed up the applicant's personal information with an offender's personal information.<sup>96</sup> Data security principles would also be relevant.<sup>97</sup> In this regard, Victorian privacy legislation provides an interesting comparison.<sup>98</sup> Under that Act, the police operate within privacy principles, subject to a few qualifications.<sup>99</sup>

### Under the UPPs

5.61 The UPPs do not provide an exemption to these particular bodies. However, the *Privacy Act 1988* (Cth) provides exemption for similar federal bodies. The ALRC were of the view that the Australian Crime Commission and the Integrity Commissioner (including the staff of the Australian Commission for Law Enforcement Integrity ("ACLEI")) – which have very similar roles and functions to the NSW equivalents –

---

91. It was held in *HW v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 214, [27] that "the meaning of the word administrative is to be read down so as not to embrace those core responsibilities".

92. Cyberspace Law and Policy Centre, *Submission*, 15; Inner City Legal Centre, *Submissions*, 31; Public Interest Advocacy Centre, *Submission*, 15: *HW v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 214 provides a good example of the misuse of operational functions.

93. This is the approach taken under the *Information Privacy Act 2000* (Vic).

94. Cyberspace Law and Policy Centre, *Submission*, 15.

95. Cyberspace Law and Policy Centre, *Submission*, 15.

96. See *OQ v Commissioner of Police* [2005] NSWADT 240.

97. Cyberspace Law and Policy Centre, *Submission*, 15.

98. *Information Privacy Act 2000* (Vic).

99. *Information Privacy Act 2000* (Vic) s 13, sch 1 IPPs 2 and 6.

required exemption from the *Privacy Act 1988* (Cth).<sup>100</sup> This was on the basis of their specialist, unique and covert role and functions, their special powers similar to those of a Royal Commission, as well as the level of oversight currently in place for the ACLEI.<sup>101</sup>

### The Commission's view

5.62 Section 27 of PPIPA and s 17 of HRIPA recognise that the Independent Commission Against Corruption, the NSW Police Force, the Police Integrity Commission and the NSW Crime Commission have a unique and important role in society – a role that may be undermined by having to comply with certain privacy principles. This role, however, ought not to be allowed to exploit privacy legislation “as a ‘secrecy’ shield, behind which government agencies may hide from proper scrutiny by other ‘watchdog’ bodies”.<sup>102</sup>

5.63 We agree with the reasoning of the ALRC that the role, function and powers of federal bodies similar to the Independent Commission Against Corruption, the Police Integrity Commission and the NSW Crime Commission warrant their exemption from privacy legislation.

5.64 However, we are of the view that there is no justification for the current level of exemption for the NSW Police Force. It will often be appropriate in circumstances to subject personal information held by the NSW Police Force to privacy principles. While it is important to recognise that their investigative and law enforcement functions are immune from privacy protection, other functions should otherwise remain subject to privacy principles.

5.65 The law enforcement and investigative functions of the Police Force would already be exempt under proposed UPPs. Additional exemption is therefore not justified.

5.66 In the event that the UPPs are not adopted in NSW, we recommend that the NSW Police Force be removed from s 27. This view is consistent with the approach under Commonwealth and Victorian legislation,<sup>103</sup> as

---

100. ALRC Report 108, vol 2, [37.43]-[37.44], [37.69]-[37.71].

101. ALRC Report 108, vol 2, [37.70].

102. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 72.

103. See respectively *Privacy Act 1988* (Cth) and *Information Privacy Act 2000* (Vic).

well as the ALRC’s recommendation that the Australian Federal Police remain subject to the privacy principles and their exceptions.<sup>104</sup>

5.67 The Independent Commission Against Corruption, the Police Integrity Commission and the NSW Crime Commission should remain exempt from PPIPA and HRIPA. For the reasons outlined above, the current level of exemption is appropriate. Any coverage of PPIPA that goes beyond the “administrative and educative functions” qualifier may cause problems in relation to those agencies’ operations. We recognise that this view is different to the recommendation made by the ALRC in respect of similar federal bodies (the Australian Crime Commission and the Australian Commission for Law Enforcement Integrity). The ALRC noted that the administrative/non-administrative dichotomy was difficult to distinguish and an impractical distinction to make.<sup>105</sup> Despite this, we are of the view that, in light of the current arrangement under PPIPA and HRIPA, and submissions we received, privacy legislation should cover the activities of agencies where possible and reasonable to do so.

5.68 We appreciate that “administrative and educative functions” may be difficult to ascertain and accordingly recommend that the Privacy Commissioner issue guidelines to assist in the interpretation of the legislation.<sup>106</sup>

#### RECOMMENDATION 5.4

Section 27 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended by excluding reference to the NSW Police Force.

#### RECOMMENDATION 5.5

The Privacy Commissioner should develop guidelines on the meaning of “administrative” and “educative” functions that will assist in the interpretation of privacy legislation.

104. ALRC Report 108, vol 2, [37.106].

105. ALRC Report 108, vol 2, [37.70].

106. The Privacy Commissioner can draw on the case law of the ADT, see *HW v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 214, [30], approved by *Commissioner of Police, New South Wales Police Force v YK (GD)* [2008] NSWADTAP 78, [20].

## 6. **Other exemptions**

- Introduction
- Courts and tribunals
- Royal commissions and special commissions
- Section 26 of PPIPA
- Named bodies
- Ministers
- Additional exemptions?

## INTRODUCTION

6.1 This chapter addresses the exemptions in the *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”) and the *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”) that have not been covered in chapters 4-5. This includes exemptions given to bodies that are identified generically or by name. Also discussed are miscellaneous exemptions and suggested new exemptions.

## COURTS AND TRIBUNALS

6.2 Section 6 of PPIPA exempts the judicial functions of courts and tribunals from the operation of that Act.<sup>1</sup> This leaves their non-judicial functions subject to PPIPA. A similar position exists under the *Privacy Act 1988* (Cth), and the Australian Law Reform Commission (“ALRC”) has recently recommended that administrative functions of courts and tribunals continue to be subject to privacy principles.<sup>2</sup>

6.3 Determining the “judicial functions” of a court or tribunal can be difficult. Sub-section 6(3) of PPIPA states that judicial functions of a court or tribunal means such of the functions of the court or tribunal as relate to the hearing or determination of proceedings before it,<sup>3</sup> and includes:

- (a) in relation to a Magistrate – such of the functions of the Magistrate as relate to the conduct of committal proceedings, and
- (b) in relation to a coroner – such of the functions of the coroner as relate to the conduct of inquests and inquiries under the *Coroners Act 1980*.

6.4 The words “relate to” in that section are to be given a broad meaning,<sup>4</sup> although there are obviously limits as to how broad this can be. Some conduct of courts and tribunals will have no connection at all, or a connection so tenuous or indirect that it does not fit into the “wide

- 
1. See also *Health Records and Information Privacy Act 2002* (NSW) s 13.
  2. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”) vol 2, [35.80].
  3. This is mirrored by the definition in the *Government Information (Public Access) Act 2009* (NSW) sch 4 cl 1.
  4. *NZ v Attorney General’s Department* [2005] NSWADT 103, [16]; see also *NZ v Director General, Attorney General’s Department* [2005] NSWADTAP 62, [8].

connection” threshold.<sup>5</sup> Given the similar wording found in the *Freedom of Information Act 1989* (NSW),<sup>6</sup> cases under that legislation may be helpful in determining the scope of s 6 of PPIPA.<sup>7</sup> The New Zealand Law Commission was of the view that “judicial functions” may include administrative tasks prior to, or some time after, the determination of a case.<sup>8</sup> This highlights the difficulty in determining when information will be in relation to “judicial functions”.

6.5 The principle of “open justice” justifies the exemption from privacy legislation of the judicial functions of courts and tribunals. It has been held to be “one of the most fundamental aspects of the system of justice in Australia”.<sup>9</sup> However, it is only a principle and “not a free standing right”.<sup>10</sup> Open justice and access to court documents may need to be limited by other considerations. Accordingly, while an important principle, open justice should not be invoked to “automatically transcend an individual’s right to privacy”.<sup>11</sup> Recognition of this consideration is becoming increasingly important with the growing influence of the Internet.<sup>12</sup>

6.6 Particular issues may arise in respect of the need for anonymity or pseudonymity, for hearings to be in camera, or for non-publication orders. While it is important for courts to conduct open forums and to make their information available to the public, courts often deal with information of a sensitive nature that individuals may want protected from others. A person may, for example, want their name to be removed

- 
5. *NZ v Attorney General’s Department* [2005] NSWADT 103, [16].
  6. Soon to be replaced by the *Government Information (Public Access) Act 2009* (NSW).
  7. See the examples given in *NZ v Attorney General’s Department* [2005] NSWADT 103, [16]-[17].
  8. New Zealand, Law Commission, *Access to Court Records*, Report 93 (2006) [2.72]-[2.74].
  9. *John Fairfax Publication Pty Ltd v District Court of New South Wales* (2004) 61 NSWLR 344, 352 (Spigelman CJ); see also J J Spigelman, “Seen to be done: the principle of open justice” (2000) 74 *Australian Law Journal* 290.
  10. *John Fairfax Publication Pty Ltd v Ryde Local Court* (2005) 62 NSWLR 512, 521 (Spigelman CJ).
  11. C Puplick, “How Far Should the Courts be Exempted from Privacy Regulation?” (2002) 40(5) *Law Society Journal* 52, 54.
  12. C Puplick, “How Far Should the Courts be Exempted from Privacy Regulation?” (2002) 40(5) *Law Society Journal* 52, 54-55.



from the case name and judgment if the appearance of their name would cause embarrassment or reveal information that is of a sensitive nature. The vast majority of privacy cases in the Administrative Decisions Tribunal (“ADT”) are of this nature. To allow for this, the *Administrative Decisions Tribunal Act 1977* (NSW) provides that names and information can be withheld if “the Tribunal is satisfied that it is desirable to do so by reason of the confidential nature of any evidence or matter or for any other reason”.<sup>13</sup>

6.7 A court relies on its inherent jurisdiction to resolve issues of this nature. Given the importance of the principle of open justice, departure from the principle is only granted in exceptional circumstances.<sup>14</sup> In *DPP v Ritson*, a case involving corrupt disclosure of the victim’s “very most private secret”,<sup>15</sup> the principle of open justice prevailed despite this highly sensitive information being revealed. Magistrate Bartley was of the view that:

The court’s implied power to sit in camera, make non-publication orders and order the use of pseudonyms did not extend to the circumstances of this case.<sup>16</sup>

6.8 The tension between privacy protection and open justice led the ADT in *NZ v Attorney General’s Department* to suggest that administrative protocols to prevent undue violations of privacy could be developed “between the Registrar, the Department, relevant Judicial Officers and the Head of Jurisdiction”.<sup>17</sup>

6.9 There is currently a consultation draft of a Court Information Bill 2009 (NSW). The draft Bill requires courts to establish practices and procedures for ensuring, “to the maximum extent reasonably practicable that the providing of access to open access information under [the

---

13. *Administrative Decisions Tribunal Act 1977* (NSW) s 75(2).

14. *John Fairfax Publication Pty Ltd v District Court of New South Wales* (2004) 61 NSWLR 344, 353. See the discussion in *Attorney-General for New South Wales v Nationwide News Pty Ltd* (2007) 72 NSWLR 635, 639-642.

15. Transcript of Proceedings, *DPP v Ritson* (Local Court, Magistrate Bartley, 12 February 2009) 10; this secret referred to the fact the victim was transgender. **The conviction in this case was overturned on appeal, after publication: *R v Ritson* [2010] NSWDC 160.**

16. Transcript of Proceedings, *DPP v Ritson* (Local Court, Magistrate Bartley, 12 February 2009) 10-11.

17. *NZ v Attorney General’s Department* [2005] NSWADT 103, [20].

proposed] Act does not facilitate access to personal identification information”.<sup>18</sup>

### *The Commission’s view*

6.10 The exemption for the judicial functions of courts and tribunals should be maintained in recognition of the principle of open justice. However, access to court information should be specifically addressed in other legislation and rules of court. We support the development of the Court Information Bill 2009 (NSW) insofar as it requires that practices and procedures be developed to assist courts to protect an individual’s personal information, to ensure that “undue violations of privacy are avoided”<sup>19</sup> – particularly in the registries, which are a part of the court.<sup>20</sup>

## ROYAL COMMISSIONS AND SPECIAL COMMISSIONS

6.11 Governments appoint Royal Commissions on an *ad hoc* basis to conduct inquiries, obtain information and report thereon.<sup>21</sup> All Australian States and the Commonwealth have legislation which confers specific powers upon Royal Commissions.<sup>22</sup> Royal Commissions may also be appointed by virtue of the prerogative power of the Crown.<sup>23</sup> Special Commissions of Inquiry have similar powers and functions to a Royal Commission; however, they are set up pursuant to the *Special Commissions of Inquiry Act 1983* (NSW).

- 
18. Court Information Bill 2009 (NSW) (Consultation Draft) cl 16(1). “Personal identification information” is defined in cl 16(4) to mean: tax file number, social security number, medicare number, financial account numbers, information in a passport, personal telephone number, date of birth (other than year of birth), home address (other than suburb, city and State or Territory), other information that can be used to establish a person’s identity and that is prescribed by the regulations as personal identification information for the purposes of this Act.
19. *NZ v Attorney General’s Department* [2005] NSWADT 103, [20].
20. *NZ v Attorney General’s Department* [2005] NSWADT 103, [14]; see also *NZ v Director General, Attorney General’s Department* [2005] NSWADTAP 62, [9].
21. See generally L Hallet, *Royal Commissions and Boards of Inquiry* (1982).
22. See, eg, *Royal Commissions Act 1902* (Cth) and *Royal Commissions Act 1923* (NSW). For discussion of the history of Royal Commissions in NSW prior to the enactment of the *Royal Commissions Act 1923* (NSW), see Justice McClemens, “The Legal Position and Procedure Before a Royal Commission” (1961) 35 *Australian Law Journal* 271.
23. L Hallet, *Royal Commissions and Boards of Inquiry* (1982) 28; *McGuinness v Attorney General (Vic)* (1940) 63 CLR 72, 93-94 (Dixon J).

6.12 A Royal Commission’s function is to investigate a matter of public concern, usually with a view to making findings of fact and issuing recommendations. In order to achieve these purposes, a Royal Commission is given a number of unique powers, including the power to compel witnesses to give evidence and produce documents<sup>24</sup> and communicate any information it receives.<sup>25</sup> Notable Royal Commissions in NSW have investigated prisons, drug trafficking, and corruption in the police service.<sup>26</sup> Notable Special Commissions of Inquiry have reported on child protection services in NSW, and the Sydney Ferries Corporation.<sup>27</sup>

6.13 Section 6 of PPIPA and s 13 of HRIPA grant an exemption to Royal Commissions and Special Commissions of Inquiry. This exemption applies to the exercise of “the Commission’s functions”.<sup>28</sup> This is a broad exemption and arguably leaves little related to a Royal Commission within the scope of PPIPA. It is unclear what (if anything) is brought under the operation of PPIPA. Further ambiguity arises in that s 4(3)(g) of PPIPA and s 5(3)(j) of HRIPA provide an exception from the definitions of “personal information” information about an individual arising out of a Royal Commission or Special Commission.<sup>29</sup> There have been no cases dealing with these provisions.

#### *The ALRC’s recommendation*

6.14 The ALRC in its review of the Royal Commission exemption under the *Privacy Act 1988* (Cth) supported a complete exemption of Royal Commissions from the application of the *Privacy Act 1988* (Cth). However, recognising the gap this created in privacy law, the ALRC

---

24. *Royal Commissions Act 1923* (NSW) s 8, s 18A.

25. *Royal Commissions Act 1923* (NSW) s 12A.

26. See respectively: JF Nagle, *Royal Commission into New South Wales Prisons* (1978); PM Woodward, *Royal Commission into Drug Trafficking* (1979); JRT Wood, *Royal Commission into the New South Wales Police Service* (1997).

27. JRT Wood, *Report of the Special Inquiry into Child Protection Services in NSW* (2008); B Walker, *Special Commission of Inquiry in Sydney Ferries Corporation* (2007).

28. *Privacy and Personal Information Protection Act 1998* (NSW) s 6.

29. We have, however, recommended that this exception be removed: see NSW Law Reform Commission, *Access to Personal Information*, Report 126 (2010) (“NSWLRC Report 126”) Recommendation 9.

recommended that guidelines should be developed so that Royal Commission's handle personal information correctly.<sup>30</sup>

*The Commission's view*

6.15 Given the importance of Royal Commissions in making findings and recommendations of significant public interest, it is vital that they are not impeded from doing so. For example, a Royal Commission should not be required to comply with collection principles because it "must be free to examine all material connected in any way with the subject matter of [its] inquiry".<sup>31</sup> Without this ability to go on a "fishing expedition", the inquiry will be hampered.<sup>32</sup>

6.16 In our view, the work of a Commission is not hampered if it is required to comply with some of the Information Protection Principles ("IPPs"). A Royal Commission may last for years and over that time may amass vast quantities of documents and information – some of which may be highly sensitive. While exemption from collection and disclosure principles will be necessary, an exemption from security principles<sup>33</sup> may not be warranted.<sup>34</sup> We are of the view that having to comply with security principles would not impair the ability of a Royal Commission to function effectively.<sup>35</sup>

6.17 Beyond this, we see merit in the ALRC's suggestion that it would be appropriate for the Privacy Commissioner to develop guidelines for Royal Commissions. Although the information collected by a Royal Commission will often be complex, sensitive or privileged, privacy guidelines will assist in ensuring the proper handling of personal information. In the interests of uniformity, these guidelines should, as far as possible, reflect those given by the Commonwealth Office of the Privacy Commissioner in relation to Commonwealth Royal Commissions.

---

30. ALRC Report 108, vol 2, [38.17]. It is to be noted that the ALRC has recently conducted an inquiry specifically related to Royal Commissions, but without any recommendation on privacy: See Australian Law Reform Commission, *Making Inquires: A New Statutory Framework*, Report 111 (2010). See also New Zealand, Law Commission, *A New Inquiries Act*, Report 102 (2008).

31. L Hallet, *Royal Commissions and Boards of Inquiry* (1982) 97.

32. L Hallet, *Royal Commissions and Boards of Inquiry* (1982) 97.

33. *Privacy and Personal Information Protection Act 1998* (NSW) s 12(c).

34. An exemption from the retention of information principle is justified given *Royal Commissions Act 1923* (NSW) s 12.

35. See para 2.29-2.32.

**RECOMMENDATION 6.1**

If the UPPs are adopted in NSW, s 6(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 13 of the *Health Records and Information Privacy Act 2002* (NSW) should be amended to require Royal Commissions or Special Commissions to be subject to UPP 8.1(a).

**RECOMMENDATION 6.2**

If the UPPs are not adopted in NSW:

- (1) s 6(2) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to require Royal Commissions or Special Commissions to be subject to s 12(c) of that Act; and
- (2) s 13 of the *Health Records and Information Privacy Act 2002* (NSW) should be amended to require Royal Commissions or Special Commissions to be subject to HPP 5(1)(c) of that Act.

**SECTION 26 OF PPIPA**

6.18 Section 26 of PPIPA provides:

- (1) A public sector agency is not required to comply with section 9 or 10 if compliance by the agency would, in the circumstances, prejudice the interests of the individual to whom the information relates.
- (2) A public sector agency is not required to comply with section 10, 18 or 19 if the individual to whom the information relates has expressly consented to the agency not complying with the principle concerned.

6.19 Sub-section 26(1) provides exemption from s 9 and s 10 which are the principles relating to collection and notification. Sub-section 26(2) provides exemption from s 10, s 18 and s 19, which are respectively the principles relating to notification, disclosure and special restrictions on disclosure.

6.20 The heading of this section curiously reads “other exemptions where non-compliance would *benefit* the individual concerned”.<sup>36</sup>

---

36. Emphasis added.

### Sub-section 26(1)

6.21 It is by no means clear when s 26(1) is applicable. HRIPA contains a provision similar to s 26(1), exempting compliance from Health Privacy Principle (“HPP”) 4 (which addresses notification) where compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates.<sup>37</sup> This provision, however, is not under a similar heading.

6.22 The title of this section suggests that the non-compliance with the relevant IPPs must be for the benefit of the individual to whom the information relates. However, it is not clear to what extent “compliance ... would ... prejudice the interests” is consistent with “non-compliance would benefit”. One suggestion has been that the provision is aimed at people with decision-making disabilities.<sup>38</sup> Thus, the provision may simply refer to a situation where collection of the information would “benefit” the individual, but the agency is unable to collect the information from that individual due to a decision-making disability.<sup>39</sup> Further, in relation to its exemption from s 10 of PPIPA, s 26(1) may cater for situations where notification to the individual would be impracticable due to a decision making disability or communicative disability, and as such, it would be more appropriate to notify a representative.<sup>40</sup> In the absence of case law, these potential applications of s 26(1) are purely speculative.

6.23 In light of the title to the provision, it would appear that s 26(1) would allow agencies to take a “paternalistic approach to determining what is in the interests of a person”.<sup>41</sup> Privacy NSW has also expressed concern that privacy standards ought to be achieved and not

---

37. *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPP 4(4)(d).

38. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 90.

39. There is also a general statement of capacity found in *Health Records and Information Privacy Act 2002* (NSW) s 7; see para 3.9.

40. Under *Health Records and Information Privacy Act 2002* (NSW) s 7(2) an individual who lacks capacity can have an authorised representative act on his or her behalf.

41. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 90.

diminished.<sup>42</sup> It was on this basis that Privacy NSW recommended that s 26(1) be repealed.<sup>43</sup>

### Sub-section 26(2)

6.24 The meaning of s 26(2) is contrastingly clear. With an individual's express consent, an agency can gain exemption from s 10, s 18 and s 19. The rationale for this provision is self-evident: if the individual authorises non-compliance with the principle, the individual's privacy is not infringed. HRIPA contains exemptions similar to s 26(2). These are contained within the relevant HPP, and provide exemptions to the HPPs relating to notification (HPP 4), use (HPP 10) and disclosure (HPP 11).<sup>44</sup> With the exception of the collection principle (IPP 2, HPP 3), the exemptions under HRIPA are the same as s 26(2) of PPIPA.

6.25 The chief requirement is that the consent be "express".<sup>45</sup> The ADT has held that even if implied consent is made out under s 26(2), it will not be enough to gain the benefit of the exemption; the legislation states that the consent must be "express".<sup>46</sup> The ADT has added that this provision ought to be strictly applied so as to maintain the beneficial nature of the legislation.<sup>47</sup>

6.26 While the rationale for the provision is self-evident, its application in respect of s 10 is questionable. Privacy NSW has argued that the application of s 26(2) in relation to s 10 is unnecessary given that, in practice, it would be easier for an agency to meet s 10 itself, rather than the exemption to it.<sup>48</sup> It makes little sense for an individual to consent to

---

42. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 90.

43. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 91.

44. Respectively: *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPP 4(4)(a); HPP 10(1)(a); HPP 11(1)(a).

45. A stricter standard than the consent requirements under the *Privacy and Personal Information Protection Act 1998* (NSW) s 18, which, arguably, could be express or implied. However, we note that the Privacy Commissioner has advised that consent should not be implied or inferred: Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities* (2004) 10.

46. *FM v Vice Chancellor, Macquarie University* [2003] NSWADT 78, [63].

47. *Vice-Chancellor, Macquarie University v FM* [2003] NSWADTAP 43, [97].

48. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 91.

not being notified: the consent itself presupposes notification. However it may be that s 26(2) intends to cover parts of the procedures set out in s 10.

## Section 26 and the proposed UPPs

6.27 The introduction of the proposed Unified Privacy Principles (“UPPs”) in NSW would largely overlap with the requirements of s 26 of PPIPA. In order to gain exemption from the IPPs listed in s 26(1) – s 9 and s 10 – the agency could rely on the “reasonable” qualifications to these UPP equivalents (UPPs 2 and 3).<sup>49</sup> For example, UPP 2.3(b) permits non-compliance with UPP 2 (Collection) when collection from the individual is not reasonable or practicable in the circumstances. On one view, it would not be reasonable to collect personal information from the individual directly if the person had a decision-making disability.<sup>50</sup>

6.28 The exemption from s 10 of PPIPA would also be covered under the UPPs. The agency under UPP 3 must inform the individual to the extent that it is reasonable to do so, or otherwise ensure that the individual is made aware of the collection. It would appear that if the individual was incapable of understanding the notification or was otherwise incapacitated, the qualifications in UPP 3 would permit that notification be given to a representative of the individual.<sup>51</sup>

6.29 In relation to s 26(2), UPP 3 (Notification) would likely cover an exemption from s 10 in the circumstance given in s 26(2). The exemptions in s 18 and s 19 of PPIPA would be covered by UPP 5.1(b) where the individual consents to the use or disclosure. There is, however, no “express” consent requirement.

## The Commission’s view

6.30 We are satisfied that on its current interpretation, s 26 would be adequately covered by the UPPs. We acknowledge that there is arguably a lower standard in place under the UPPs relating to consent for use and disclosure. Under the UPPs “express” consent is not required, leaving open the question whether implied consent is sufficient.<sup>52</sup> Despite this

---

49. See para 5.23-5.30.

50. See Chapter 3.

51. See Chapter 3.

52. Although the Privacy Commissioner has advised that consent should not be implied or inferred under the *Privacy and Personal Information Protection Act 1998*



difference, in the interests of maintaining uniformity, we have supported the adoption of the UPPs in their current form and consequently recommend the repeal of s 26.

6.31 In the event that the UPPs are not adopted in NSW, we recommend that s 26(1) of PPIPA and HPP 4(4)(d) be repealed as we can see no point to them. There is little indication that s 26(2) is problematic and accordingly we do not make any recommendations with respect to this provision.

### RECOMMENDATION 6.3

If the UPPs are adopted in NSW, s 26 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

### RECOMMENDATION 6.4

If the UPPs are not adopted in NSW s 26(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) and HPP 4(4)(d) of the *Health Records and Information Privacy Act 2002* (NSW) should be repealed.

## NAMED BODIES

6.32 Under s 28(1) of PPIPA, the Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Guardianship Board<sup>53</sup> are not required to comply with s 19.<sup>54</sup> HPPs 10(3) and 11(3) provide a similar exemption, but differ in that the exception to use and disclosure of any information applies only in relation to the named bodies' "complaint handling functions and their investigative, review and reporting functions".

### Under the UPPs

6.33 The UPPs would overlap with s 28(1) as it relates to the sensitive information listed in s 19(1). In order for the bodies named in s 28(1) to gain the benefit of the exemption under UPP 5, they will have to satisfy

---

(NSW): Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities* (2004) 10.

53. The Guardianship Tribunal "is the same entity as, and a continuation of, the former [Guardianship Board]": *Guardianship Act 1987* (NSW) sch 3 cl 3.

54. *Privacy and Personal Information Protection Act 1998* (NSW) s 28(1).

one of the exceptions within that UPP. Ostensibly, this is a more restrictive exemption than the bodies listed in s 28(1) currently have under PPIPA. However, the UPPs do not make special exceptions for the use and disclosure of sensitive information, except insofar as UPP 5.1(a) applies.<sup>55</sup> On this basis, the Ombudsman's Office, the Health Care Complaints Commission, the Anti-Discrimination Board and the Guardianship Board will be able to use and disclose sensitive information of the sort referred to in s 19(1) if they satisfy any of the exception criteria under UPP 5.

6.34 UPP 5 describes the circumstances in which personal information may be used or disclosed for a secondary purpose. Without detailing the stricter requirement for disclosing sensitive information under UPP 5.1, sensitive information may be used or disclosed for a secondary purpose in the other listed circumstances, for example if "required or authorised by or under law" (UPP 5.1(e)). Further, the bodies listed in s 28(1) would fall under the recommended definition of "enforcement body"<sup>56</sup> and would thus qualify for the exceptions relating to enforcement bodies.<sup>57</sup> The exceptions to UPP 5 would also cover HPPs 10(3) and 11(3).

### The Commission's view

6.35 We are satisfied that the current exemption under PPIPA would effectively be maintained under the proposed UPPs. As a result, s 28(1) of PPIPA and HPPs 10(3) and 11(3) should be repealed if the UPPs are adopted. With regard to the role and requirements of the Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Guardianship Board, a complete exemption from s 19(1) is necessary and justified. Consequently, we do not recommend any changes in respect of s 28(1) if the UPPs are not adopted.

---

55. Under UPP 5.1(a) "[a]n agency or organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection (the secondary purpose) unless ... the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection".

56. See Recommendations 5.1-5.2.

57. See Chapter 5.

## RECOMMENDATION 6.5

If the UPPs are adopted in NSW, s 28(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) and HPPs 10(3) and 11(3) of the *Health Records and Information Privacy Act 2002* (NSW) should be repealed.

## MINISTERS

6.36 Section 28(3) exempts any agency from compliance with s 17, s 18 and s 19 of PPIPA if the disclosure is for the purpose of informing the Minister of that agency or the Premier about any matter.<sup>58</sup> There is a similar exemption in HRIPA under HPPs 10(4) and 11(4) where a general exception to use and disclosure principles is given to agencies for the purpose of informing the Minister of that agency or the Premier about any matter. There is no equivalent provision under the UPPs.

6.37 Privacy NSW has recommended that s 28(3) be amended so as to reduce its currently broad application. It has argued that the current scope of s 28(3) would allow the disclosure of personal information for “any reason whatsoever”.<sup>59</sup> The Premier may seek, for example, the criminal history of powerful public figures, and the information then disclosed would no longer be subject to PPIPA. Victims of misuse would have no recourse under privacy legislation. There could, in the view of Privacy NSW, be no justification for a provision this broad. Under Victorian Legislation, a Minister is subject to the *Information Privacy Act 2000*.<sup>60</sup> The Minister is subject to the IPPs and would have to rely on the normal exceptions to them.

6.38 The recommendation of Privacy NSW was to reduce the ambit of this provision so as to apply only to what is reasonably necessary for the Minister to perform ministerial functions.

### The Commission’s view

6.39 It is important that, for the proper exercise of their portfolios, Ministers and the Premier are able to make important decisions on the basis of proper up-to-date information. They should be able to discuss

58. *Privacy and Personal Information Protection Act 1998* (NSW) s 28(3).

59. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 91.

60. *Information Privacy Act 2000* (Vic) s 9(1)(a).

these matters freely in order to be satisfied as to the appropriateness of their decisions. However, we agree with Privacy NSW that this provision is too broadly formulated. The underlying purpose of this provision could still be attained if its ambit was narrowed.

6.40 In order to ensure that the personal information requested by Ministers and the Premier is for a legitimate purpose and will be used in good faith, we support Privacy NSW's suggested amendment that the disclosure be "reasonably necessary for the minister to perform the ministerial functions relating to that portfolio or agency".<sup>61</sup> We acknowledge that in practice this may be difficult to demonstrate. However, in the interests of preventing "information laundering" or misuse of personal information, we believe that this change is justified.

#### RECOMMENDATION 6.6

Section 28(3) of the *Privacy and Personal Information Protection Act 1998* (NSW) and HPPs 10(4) and 11(4) of the *Health Records and Information Privacy Act 2002* (NSW) should be amended to apply where the disclosure is reasonably necessary for the Minister or Premier to perform the ministerial functions relating to that portfolio or agency.

## ADDITIONAL EXEMPTIONS?

### Alternative dispute resolution

6.41 There is no exemption in PPIPA for Alternative Dispute Resolution ("ADR"). The proposed UPPs provide for new exceptions in relation to collection and use and disclosure principles where the personal information is for the purpose of a confidential process of ADR. This includes the collection, use and disclosure of sensitive information.<sup>62</sup> This was in recognition of the critical role of ADR in the effective, efficient and fair resolution of disputes.

6.42 The ALRC has discussed at length the reasons for introducing this exception. In Report 123, we expressed agreement with this exception on the basis that ADR has become an essential and common element in the

61. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 92.

62. UPPs 2.5(g) and 5.1(h).

resolution of disputes in Australia.<sup>63</sup> As a result, we recommend that, if the UPPs are not adopted in NSW, a similar provision be included in PPIPA. In accordance with the ALRC's recommendations, this new exception in PPIPA should provide an exception from s 8, s 17, s 18 and s 19(1) of PPIPA.

6.43 Further, in the interests of uniformity, we recommend that this new provision should provide that public sector agencies need not comply with s 8, s 17, s 18 and s 19(1) where non-compliance is necessary for the purpose of a confidential alternative dispute resolution process. This mirrors the wording used under the proposed UPPs.

#### RECOMMENDATION 6.7

If the UPPs are not adopted in NSW, the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that a public sector agency need not comply with s 8, s 17, s 18 and s 19(1) where non-compliance is necessary for the purpose of a confidential alternative dispute resolution process.

#### Suitability for appointment or employment as a public sector official

6.44 Paragraph 4(3)(j) of PPIPA and s 5(3)(m) of HRIPA exempt from the definition of personal information "information or an opinion about an individual's suitability for employment as a public sector official". In Report 126 we recommended that this exemption be repealed.<sup>64</sup> We left open the question whether a more limited exemption be contained in privacy legislation as a specific exemption to certain IPPs or HPPs.

6.45 In our view, there is no compelling justification for the creation of a specific exemption for the purpose of determining the suitability for appointment or employment as a public sector official. Employee records should be subject to normal privacy principles and exemptions to those principles, for example, the "required or authorised by or under law" exemption, and those in relation to investigation of misconduct. Exemption to the IPPs and HPPs can also be gained by obtaining the individual's consent to use or disclose personal information (including sensitive information). Further, employees should, in most situations, be

63. NSW Law Reform Commission, *Privacy Principles*, Report 123 (2009) [2.136]-[2.147].

64. See NSWLRC Report 126, Recommendation 9.

able to access their personal information. This view is consistent with the ALRC's recommendations in relation to a similar exemption for private sector organisations.<sup>65</sup>

6.46 We agree with the ALRC that there is no sound policy reason why there should be a difference in the coverage between the private and public sectors.<sup>66</sup> It is therefore important that there be consistency in information handling, whether the employer is an agency or organisation.

6.47 The proposed UPPs would adequately address the concerns of some stakeholders that the removal of the exception may negatively impact on employee misconduct investigations or duties of confidentiality.<sup>67</sup> It was argued that providing access in these circumstances should not be required, as it may dissuade colleagues from making reports of misconduct,<sup>68</sup> or discourage referees from making full and frank disclosure.<sup>69</sup> With regard to information about employees' suitability for employment, we agree with the ALRC's view that UPP 9 (Access and Correction) strikes an appropriate balance between providing access to employees and allowing employers to deny access in appropriate circumstances.<sup>70</sup> More generally, we agree with the reasoning of the ALRC that the qualifications and exceptions to the UPPs will address employees' concerns.<sup>71</sup>

6.48 If the UPPs are not adopted in NSW, we maintain our view that a specific exemption for employee records is unwarranted.<sup>72</sup> As a form of personal information (potentially including sensitive information), the current exemptions from PPIPA, as well as the recommendations in this report, achieve the appropriate level of protection.

---

65. ALRC Report 108, vol 2, ch 40 generally.

66. ALRC Report 108, vol 2, [40.96].

67. ALRC Report 108, vol 2, [40.136]-[40.150].

68. National Australia Bank, *Submission PR 408 to the ALRC*, 7 December 2007, cited in ALRC Report 108, vol 2, [40.144]-[40.145].

69. Suncorp-Metway Ltd, *Submission PR 525 to the ALRC*, 21 December 2007, cited in ALRC Report 108, vol 2, [40.141].

70. ALRC Report 108, vol 2, [40.154].

71. ALRC Report 108, vol 2, ch 40 generally.

72. See NSWLRC Report 126, [2.78].

## Part 8A of the Police Act 1990 (NSW)

6.49 Information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990* (NSW) is exempt from the definition of personal information.<sup>73</sup> In Report 126 we recommended the repeal of this exemption, but expressed the provisional view that it should be included as a specific exemption in PPIPA, where it can be exempted from the application of relevant privacy principles.<sup>74</sup> Part 8A of the *Police Act 1990* (NSW) provides the procedures for investigating complaints against a police officer. NSW Police have submitted that it requires broad powers in respect of investigating matters of police misconduct.<sup>75</sup>

6.50 In a number of ways, the proposed UPPs exempt from privacy principles an investigation conducted by an “enforcement body”.<sup>76</sup> UPP 5.1(f)(iv) is relevant.<sup>77</sup> In other circumstances UPP 5.1(d) may apply. Other exemptions could be gained by relying on the reasonableness exceptions to the principles, for example UPP 3 (Notification). The ALRC has commented that it would not be reasonable “to require an employer to notify the employee who is the subject of the complaint if the complaint was not substantive enough to warrant further investigation”.<sup>78</sup> Similarly, notification would not be reasonable if to do so would prejudice an investigation into an employee’s misconduct.<sup>79</sup> Similar reasoning is applicable to the “Collection” or “Access and Correction” UPPs.<sup>80</sup>

6.51 Under the proposed UPPs, information used or disclosed which is not relevant to a complaint, or which the agency does not reasonably believe is necessary for the investigation, will not be protected by the exemption in UPP 5.1(d) or (f)(iv). Therefore, information used or disclosed which has an “indeterminate or tenuous” relationship to a

---

73. *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(h); *Health Records and Information Privacy Act 2002* (NSW) s 5(3)(k).

74. See NSWLRC Report 126, [2.87].

75. Statutory Review of PPIPA, [9.26].

76. See Chapter 5.

77. “[T]he prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct.”

78. ALRC Report 108, vol 2, [40.157].

79. ALRC Report 108, vol 2, [40.157].

80. Depending on the circumstances, it may be appropriate to deny access to complainants or the individual subject to the complaint.

complaint or investigation will be subject to normal privacy principles.<sup>81</sup> This is similar to the current position under s 4(3)(h) of PPIPA and s 5(3)(k) of HRIPA.<sup>82</sup>

6.52 There is also the protection offered to complainants by way of a prohibition on the disclosure of the identity of a complainant. This is provided in s 169A of the *Police Act 1990* (NSW) and will enliven the “required or authorised by law” exemption.

6.53 Under the proposed UPPs, the threshold for the exception to “use and disclosure” principles under UPP 5.1(d) (as modified in Report 123),<sup>83</sup> is suspicion of “serious misconduct”; or under UPP 5.1(f), “serious improper conduct or prescribed conduct”. This threshold may not include some of the conduct listed in s 122 of the *Police Act 1990* (NSW),<sup>84</sup> for example a mistake of fact or law. Although regulations may prescribe exempt conduct to include conduct listed in s 122 of the *Police Act 1990* (NSW), currently under the UPPs there will be some complaints which do not get the benefit of the exception.

6.54 It appears, therefore, that the UPPs would not address all the circumstances to which Part 8A relates. In the interest of facilitating investigations into police misconduct, we recommend that the exemption in relation to information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990* (NSW) be included as a specific exemption. It is clear that investigations of this nature are an appropriate and efficient way of dealing with complaints. Moreover, the Ombudsman plays an oversight (or possibly active) role in respect of Part 8A investigations.<sup>85</sup> This justifies the proposed exemption.

6.55 If the UPPs are not adopted in NSW, we recommend the creation of a specific exemption in relation to complaints against a police officer. Our

---

81. *KO v Commissioner of Police* [2004] NSWADTAP 21, [32].

82. See *GA v Department of Education and Training* [2004] NSWADTAP 18, [55].

83. NSW Law Reform Commission, *Privacy Principles*, Report 123 (2009) Recommendation 6.

84. This section includes conduct that is an offence, corrupt, unlawful, unreasonable, unjust, oppressive, or conduct that arises from improper motives or irrelevant considerations, from a mistake of fact or law or conduct of a kind for which reasons should have (but have not) been given.

85. *Police Act 1990* (NSW) s 140.



recommendations in respect of “investigative agencies”,<sup>86</sup> while flexible, may not allow for non-compliance with privacy principles in relation to all the types conduct of a police officer listed in s 122 of the *Police Act 1990* (NSW). The reasoning above in relation to Part 8A investigations under the proposed UPPs can be applied to “investigative agencies”, where there are similar “reasonable”, “practicable” or more specific exemptions in place.

#### RECOMMENDATION 6.8

---

The *Privacy and Personal Information Act 1998* (NSW) should include a specific exemption relating to information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990* (NSW).

---

86. See Recommendations 5.1-5.5

## 7. **Regulatory instruments**

- Introduction
- Regulations
- Privacy codes of practice
- Public interest directions

## INTRODUCTION

7.1 This chapter deals with the ways that other instruments – regulations, privacy codes and public interest directions (“PIDs”) – can modify, interpret or add to the privacy principles. The workings of the current regulatory scheme under the *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”) are unclear and in many respects confusing and thus require clarification. We have outlined some of the problems in Consultation Paper 3 (“CP 3”).<sup>1</sup> This chapter recommends a complete overhaul of the co-regulation scheme in line with the ALRC recommendations.

7.2 Essentially, the current scheme has three methods of doing the same thing. Regulations, codes and PIDs are all used to make detailed, long-term exemptions from various privacy principles.<sup>2</sup> The choice between these options is confusing for many agencies and leads to delays and a lack of flexibility in crafting necessary exemptions or clarifications. Further, in some cases, there is a lack of transparency and accountability in the process of creating an exemption. For example, one stakeholder, in the process of attempting to facilitate an inter-agency information sharing program was advised halfway through the application process for a PID that a PID was not available. One of the reasons for this was because the nature of the program was long-term and therefore required a code. This resulted in the further suspension of the program while a code was drafted, instead of a PID being used to allow the program to continue during the code-drafting process.<sup>3</sup>

7.3 We thus recommend a scheme where each of these instruments plays a different and supporting role. In outline, large scale or permanent exemptions from the privacy principles will be made wherever possible by legislative amendment. Where more flexibility in specifically defined circumstances is required, regulations will be used. Privacy codes will be used to “modify” and interpret, but not “regulate”, the application of the privacy principles. This will mean that they cannot decrease the privacy

- 
1. NSW Law Reform Commission, *Privacy Legislation in New South Wales*, Consultation Paper 3 (2008) (“NSWLRC CP 3”) Proposal 17, Issues 48, 49 and 52.
  2. Note that public interest directions are meant to function temporarily: see discussion below at para 7.67.
  3. NSW Department of Justice and Attorney General, Crime Prevention Division, *Consultation*.

protection afforded overall, but can provide detailed guidelines on how specific agencies or programs will deal with privacy issues. PIDs will be used as temporary measures while a code or regulation is being developed. They will be able to decrease the privacy protection afforded by the Act, but only in the short-term.

## REGULATIONS

7.4 The Governor has power to make regulations “exempting specified persons or public sector agencies, or classes of persons or public sector agencies” from the requirements of PPIPA relating to collection, use or disclosure or specified classes of personal information or any provision of PPIPA.<sup>4</sup> Regulations made under this power are statutory rules<sup>5</sup> and thus subject to disallowance by Parliament.<sup>6</sup> Regulations must not be inconsistent with the Act.<sup>7</sup>

7.5 To date, there has only been one regulation created under this power, renewed in 2005.<sup>8</sup> The Statutory Review of PPIPA notes that the

- 
4. *Privacy and Personal Information Protection Act 1998* (NSW) s 71. The same applies to the *Health Records and Information Privacy Act 2002* (NSW) s 75. Note that regulations can also be used for other purposes: to define certain terms, such as “investigative agency”, “law enforcement agency”, “personal information”, and so on (s 3); to prescribe procedures for internal review (s 53(3)(e)); or to define “authorised persons” under s 44.
  5. *Subordinate Legislation Act 1989* (NSW) s 3.
  6. *Interpretation Act 1987* (NSW) s 41.
  7. *Privacy and Personal Information Protection Act 1998* (NSW) s 71(1). See also Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”) vol 1, [5.59]-[5.62].
  8. *Privacy and Personal Information Protection Regulation 2005* (NSW), which replaced the *Privacy and Personal Information Protection Regulation 2000* (NSW). The regulation does five things: (a) it exempts art, publicly available State records under the *State Records Act 1998* (NSW) and archived information from the definition of “personal information”, bringing the definition in line with the *Health Records and Information Privacy Act 2002* (NSW); (b) it exempts agencies that are included within another agency from the necessity of creating a privacy management plan under the *Privacy and Personal Information Protection Act 1998* (NSW) s 33; (c) it exempts certain registers (discussed in Chapter 8) from the provisions of the *Privacy and Personal Information Protection Act 1998* (NSW) pt 6 relating to disclosure; (d) it completely exempts the Council of the Law Society and the Council of the Bar Association from all the provisions of the *Privacy and Personal Information Protection Act 1998* (NSW); and (e) it exempts from disclosure requirements the Department of Aboriginal Affairs, the State Records

full scope of the regulation-making power “does not appear to have been explored, possibly because of the other methods available to agencies for modifying the [Information Protection Principles]” (“IPPs”).<sup>9</sup>

### Issues raised by the regulation-making power

7.6 Section 100 of the *Privacy Act 1988* (Cth) empowers the Governor-General to make regulations:

- (1) ...not inconsistent with this Act, prescribing matters:
  - (a) required or permitted by this Act to be prescribed; or
  - (b) necessary or convenient to be prescribed for the carrying out or giving effect to this Act.

7.7 This includes prescribing organisations and identifiers to which National Privacy Principle (“NPP”) 7.1 does not apply, and allowing derogations from those principles.<sup>10</sup> The regulation-making process includes a consultation requirement, which would likely involve the Commonwealth Privacy Commissioner.<sup>11</sup>

7.8 The Australian Law Reform Commission (“ALRC”) noted that “matters subject to frequent change” may be dealt with by regulation, as well as more specific matters than are dealt with in the legislation.<sup>12</sup>

7.9 The submissions to the ALRC were divided on whether regulations were suited to being the primary method of modifying the privacy principles. The Office of the Commonwealth Privacy Commissioner and Telstra raised the issue of the propriety of allowing regulations to derogate from legislative standards, and submitted that for the purposes

---

Authority and the Premier’s Department from collection, holding, use and disclosure IPPs in respect to the Aboriginal Trust Funds Repayment Scheme, and any other public agency disclosing information to these specific agencies.

9. NSW Attorney General’s Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly) (“Statutory Review of PPIPA”) [11.5].
10. *Privacy Act 1988* (Cth) sch 3 NPP 7.1A, s 100(2). See also ALRC Report 108, vol 1, [4.43].
11. ALRC Report 108, vol 1, [4.44]; *Legislative Instruments Act 2003* (Cth) s 17-19.
12. ALRC Report 108, vol 1, [4.43], [5.60].

of accountability, certainty and consistency, significant changes should be achieved only through legislation.<sup>13</sup>

7.10 The Public Interest Advocacy Centre raised the concern of “repeal by instalment”; that is, the erosion of privacy protection through subordinate legislation,<sup>14</sup> which has also been raised by the Australian Privacy Foundation with respect to privacy codes and PIDs under NSW privacy legislation.<sup>15</sup>

7.11 The Statutory Review of PPIPA recommended that:

Exemptions in existing codes and directions should be included in the Act or in Regulations. Future variations to the application of the Act should be by way of regulation only. Provision for consultation with the Privacy Commissioner prior to the making of a regulation should be made.<sup>16</sup>

7.12 The NSW Government in their response to the Statutory Review raised the concern that regulations may, in fact, not be flexible enough to respond to “emerging and unforeseen projects and developments”.<sup>17</sup>

### The Commission’s view

7.13 Since regulations are disallowable instruments, we recommend, subject to certain clarifications, that they be the main instrument by which modifications, especially abrogations, of the privacy principles are achieved. For example, regulations could be used where exemptions are too specific to be contained in the relevant legislation. This is in line with the structural model recommended by the ALRC.<sup>18</sup> While we note that the Commonwealth Government has not accepted the ALRC’s

---

13. ALRC Report 108, vol 1, [5.51]-[5.52].

14. ALRC Report 108, vol 1, [5.54], quoting Public Interest Advocacy Centre, *Submission PR 548 to the ALRC*, 26 December 2007.

15. Australian Privacy Foundation, *Submission to the NSW Attorney General’s Department Review of the Privacy and Personal Information Protection Act 1998* (2004) 7.

16. Statutory Review of PPIPA, Recommendation 21.

17. NSW Government, *Response to the Report on the Statutory Review of the Privacy and Personal Information Protection Act 1998* (“NSW Government Response to the Statutory Review”) 10. Google Australia submitted that a “flexible approach to regulation is essential”. Google Australia, *Submission PR 539 to the ALRC*, 21 December 2007, quoted in ALRC Report 108, vol 1, [5.57].

18. ALRC Report 108, vol 1, ch 4, specifically [4.42]-[4.44].

recommendation with regard to regulations, their response is in line with our general approach.<sup>19</sup> We agree with the Statutory Review of PPIPA's recommendation for consultation with the Privacy Commissioner prior to the making of a regulation, and note that s 5 of the *Subordinate Legislation Act 1989* (NSW) requires that submissions be invited on proposed regulations and that these submissions are to be appropriately considered. In Report 125 we recommend that "[t]he Minister should be required to consult with the Information Commissioner before creating regulations pursuant to privacy legislation".<sup>20</sup> If the model we propose in Report 125 is not adopted, regulations pursuant to PPIPA should be made after consultation with the Privacy Commissioner.

7.14 We acknowledge the concerns raised that regulations will be too inflexible a method of derogation, but also note that the majority of submissions were in fact in favour of a stricter approach to lowering privacy standards. Where general or significant exemption from PPIPA is required, we agree with the Commonwealth Government that this should be achieved through amendment of the legislation. The issue of short-term flexibility can be addressed through the use of PIDs, which can provide some breathing space while a regulation is developed. We believe that this approach to regulations is a compromise that balances flexibility and privacy effectively.

#### RECOMMENDATION 7.1

Regulations should be the main method of imposing on agencies different or more specific privacy requirements that are still consistent with the overall purposes of the *Privacy and Personal Information Protection Act 1998* (NSW).

- 
19. Australian Government, *Enhancing National Privacy Protection*, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 *For Your Information: Australian Privacy Law and Practice* (2009) 21.
  20. NSW Law Reform Commission, *The Offices of the Information and Privacy Commissioners*, Report 125 (2009) ("NSWLRC Report 125") Recommendation 10. This is in line with our recommendations in NSW Law Reform Commission, *Access to Personal Information*, Report 126 (2010), ("NSWLRC Report 126") Recommendation 9.

**RECOMMENDATION 7.2**

If Recommendation 10 in Report 125 is not adopted, regulations pursuant to the *Privacy and Personal Information Protection Act 1998* (NSW) should be made after consultation with the Privacy Commissioner.

**PRIVACY CODES OF PRACTICE**

7.15 Codes of practice are widely used in privacy and data protection laws around the world, in varying forms and for diverse purposes. The *Privacy Act 1988* (Cth),<sup>21</sup> PPIPA<sup>22</sup> and its equivalent in Victoria,<sup>23</sup> all provide for the making of codes, as does the *Privacy Act 1993* (NZ).<sup>24</sup> The advantage of codes and rules applying to particular public and private sector organisations or industry groups is that they can be crafted to meet specific needs and practices.<sup>25</sup> The ability to make codes also allows for greater flexibility to deal with the emergence of a clearly defined privacy risk, and to accommodate developing technologies.<sup>26</sup> Further, codes of practice have an advantage over regulations as they generally allow the involvement of industry and the public in consultation and the development of rules.<sup>27</sup>

7.16 However, if codes of practice fail to have adequate oversight and consultation with relevant stakeholders, they can lessen Parliamentary control over the setting of legal standards, and can be used to avoid laws that would better protect public or individual interests. They can also take a long time to develop if adequate oversight and consultation mechanisms are in place.<sup>28</sup> In NSW, there has been some concern that the difficult and lengthy process required to develop codes has discouraged effective use of codes and also that codes are being used to entrench

21. *Privacy Act 1988* (Cth) pt 3AA.

22. *Privacy and Personal Information Protection Act 1998* (NSW) pt 3.

23. *Information Privacy Act 2000* (Vic) pt 4.

24. See *Privacy Act 1993* (NZ) pt 6.

25. Office of the Victorian Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy (Issues Paper No 31)* (2007) [144], [179].

26. Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Discussion Paper 72* (2007) 26.

27. Note, however, that this is not currently the case in NSW.

28. Office of the New Zealand Privacy Commissioner, *Necessary and Desirable – Privacy Act 1993 Review* (1998) [6.1.10].



broad, long term variations, which are better made with Parliamentary scrutiny:<sup>29</sup>

The Act is weak in some places; for example, by adopting a code of conduct a Minister can avoid a number of requirements of the Act ... [t]he legislation is capable of some amendment and improvement, particularly in relation to codes of practice.<sup>30</sup>

7.17 This section surveys the role of privacy codes generally in the Commonwealth as well as in State and Territory jurisdictions and then turns to evaluate their operation in NSW and whether the particular issues raised by codes currently in place can be accommodated by legislative or other means.

## New South Wales

### *Operation of privacy codes of practice*

7.18 In NSW, Part 3, Division 1 of PPIPA allows for the making of privacy codes of practice. Under Part 3, codes of practice may be made for the purposes of protecting the privacy of the individual. These codes of practice may “regulate collection, use and disclosure” of personal information, and prescribe procedures for dealing with information held by public sector agencies.<sup>31</sup> Under s 30(1), codes may also “modify the application” of any one or more of the IPPs or Part 6 (relating to public registers).

7.19 Codes may provide protection for personal information contained in a record that is more than 30 years old (but must be consistent with the *State Records Act 1998* (NSW)). Codes may provide for disclosure of personal information to people or bodies outside NSW, and can apply to a specified class of personal information, public sector agency or activity or class of activity.<sup>32</sup>

7.20 Unlike the Commonwealth code provisions, PPIPA only allows for the development of codes that decrease the privacy protection granted by the IPPs. When the Privacy and Personal Information Protection Bill 1998 was first introduced in Parliament, it contained a provision conferring on

---

29. Australian Privacy Foundation, *Submission*, 11.

30. New South Wales, *Parliamentary Debates*, Legislative Assembly, 29 October 2003, 4401 (A Tink, Shadow Attorney General).

31. *Privacy and Personal Information Protection Act 1998* (NSW) s 29(1)-29(2).

32. *Privacy and Personal Information Protection Act 1998* (NSW) s 29(3)-29(5).

the Privacy Commissioner the power to veto a code that sought to exempt a public sector agency from compliance with an IPP. However, this power was removed by amendment in the Bill's committee stage.<sup>33</sup> PPIPA in its current form states that codes must "provide standards of privacy protection that operate to protect public sector agencies from any restrictions in relation to the importation of personal information into New South Wales" and *must not* impose requirements that are more stringent or of a higher standard than the IPPs.<sup>34</sup> Further, codes cannot affect the operation of any exemption contained in Division 3, Part 2.<sup>35</sup> Codes can not only specify different requirements to those in the IPPs and exempt any activity or conduct of or by the public sector agency from compliance, but can also specify how a public sector agency will apply or follow the IPPs. Codes can also exempt a public sector agency or class of agencies from compliance with the IPPs.<sup>36</sup>

7.21 A former NSW Privacy Commissioner has commented that as the IPPs are somewhat more restrictive than the Commonwealth privacy principles, the opportunities for modifying the principles are broader.<sup>37</sup>

#### *Preparation and making of privacy codes of practice*

7.22 The Privacy Commissioner or any public sector agency (in consultation with the Privacy Commissioner) can initiate, develop and submit a draft code to the Minister (Attorney General). The Privacy Commissioner can make submissions to the Minister regarding the draft code. Upon submission and after taking into considerations submissions from the Privacy Commissioner the Minister may decide to make the code.<sup>38</sup> A code of practice is made by order of the Minister published in *The Gazette*. A code takes effect when the order making the code is published (unless a later date is specified in the order). The procedures

---

33. NSW, *Parliamentary Debates*, Legislative Assembly, 18 November 1998, 10278-10279; see also NSW, *Parliamentary Debates*, Legislative Council, 25 November 1998, 10592-10593.

34. *Privacy and Personal Information Protection Act 1998* (NSW) s 29(7).

35. *Privacy and Personal Information Protection Act 1998* (NSW) s 29(6).

36. *Privacy and Personal Information Protection Act 1998* (NSW) s 30(2).

37. C Puplick, "Codes and Consultation in NSW" (2000) 7(3) *Privacy Law and Policy Reporter* 53.

38. Compare the relevant Commonwealth provision where the Privacy Commissioner has the power to approve privacy codes: *Privacy Act 1988* (Cth) s 18BB.

outlined in this section extend to any amendment of a privacy code of practice.<sup>39</sup>

### *Compliance with codes*

7.23 An agency must comply with any code of practice that applies to that agency. Contravention of a code is conduct to which Part 5 (relating to internal review) applies.<sup>40</sup> A complaint can also be lodged with the Privacy Commissioner under s 45 of PPIPA.

### *Health privacy codes of practice*

7.24 The same ability to make codes exists under Part 5 of the *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”). As of the time of writing, only one health code has been created.<sup>41</sup> According to its explanatory note, it is intended to permit, 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 information relates. It is analogous to the “Human Services” part of the General Code<sup>42</sup> and the same criteria apply.

## Commonwealth privacy codes

7.25 The Commonwealth Privacy Commissioner has various powers in relation to privacy codes (applying to organisations) under the *Privacy Act 1988* (Cth). The Commonwealth Privacy Commissioner has the power to:

- approve codes and variations to existing codes as well as to revoke those approvals;<sup>43</sup>
- review the operation of approved privacy codes;<sup>44</sup>
- prepare and publish guidelines about the development, approval and variation of privacy codes and complaint handling processes under these codes;<sup>45</sup> and

39. *Privacy and Personal Information Protection Act 1998* (NSW) s 31.

40. *Privacy and Personal Information Protection Act 1998* (NSW) s 32.

41. The *Health Records and Information Privacy Code of Practice 2005* (NSW).

42. See para 7.41, 7.58 and Appendix B.

43. *Privacy Act 1988* (Cth) s 27(1)(aa).

44. *Privacy Act 1988* (Cth) s 27(1)(ad), s 18BI.

45. *Privacy Act 1988* (Cth) s 27(1)(ea).

- consider applications for review of determinations of adjudicators in relation to a complaint under the code.<sup>46</sup>

7.26 In order for a code to be approved, the Commonwealth Privacy Commissioner must be satisfied that the code incorporates all the NPPs or sets out obligations which are, overall, at least equivalent to the NPPs.<sup>47</sup> Currently, there are three industry codes.<sup>48</sup>

7.27 The ALRC has recommended that the *Privacy Act 1988* (Cth) be amended to specify that a privacy code should operate in addition to the proposed model Unified Privacy Principles (“UPPs”), and does not replace the UPPs.<sup>49</sup> The codes may provide guidance or standards on how organisations bound by the code are to comply with one or more of the UPPs as long as such guidance contains obligations that, overall, are at least equivalent to the obligations set out in the UPPs.<sup>50</sup>

### Other Australian jurisdictions

7.28 The *Information Privacy Act 2000* (Vic) (“IPA”) provides that an organisation can discharge its duty to comply with an IPP in respect of personal information it has collected, held, used or disclosed by complying with a code of practice approved under the Act. Like the *Privacy Act 1988* (Cth), the Victorian scheme allows approved codes of practice to set standards for information handling that differ from the default scheme as long as the standards are at least as stringent as those prescribed by any IPP. They may also prescribe how any one or more of the privacy principles are to be applied, or are to be complied with.<sup>51</sup>

7.29 The Victorian Privacy Commissioner, before deciding whether to advise the Attorney to approve a code, may consult with any person he or she considers appropriate and must have regard to the extent the public has been given the opportunity to comment on the proposed

---

46. *Privacy Act 1988* (Cth) s 27(1)(ae), s 18BI.

47. *Privacy Act 1988* (Cth) s 18BB(2)(a).

48. These are the “Market and Social Research Privacy Code”, the “Queensland Club Industry Privacy Code” and the “Biometrics Institute Privacy Code”. Note further that Commonwealth privacy codes differ to NSW privacy codes in that they apply only to organisations, not to public sector agencies. The adoption of the UPPs will change this.

49. ALRC Report 108, vol 2, Recommendation 48-1.

50. ALRC Report 108, vol 2, Recommendation 48-1.

51. *Information Privacy Act 2000* (Vic) s 18.

code.<sup>52</sup> There have been no codes made under the IPA since it came into force in 2001.<sup>53</sup>

7.30 The new Queensland privacy legislation does not include provisions for the development of codes of practice. Rather, it relies on exemptions contained specifically in the Act, and also public interest waivers and modifications (“approvals”) as determined by the Information Commissioner.<sup>54</sup> These operate similarly to PIDs, but s 157 approvals must be tabled in Parliament and are disallowable instruments.<sup>55</sup>

### Clarification of the scope of codes of practice

7.31 The main concern with privacy codes of practice as they stand is the fact that they can reduce the privacy protection granted by the IPPs.<sup>56</sup> This leads to a wide variety of exemptions that are not open or transparent. In turn, this generates two main problems:

- confusion as to the responsibilities and duties of any particular agency, both for the agency and for the general public.<sup>57</sup>
- derogation from legislative privacy standards without transparency or proper accountability measures.<sup>58</sup>

7.32 As we have noted in Report 123, “privacy regulation will only remain effective if regulations clarify and strengthen, not dilute, the default standards set in privacy principles”.<sup>59</sup>

7.33 The Statutory Review of PPIPA has summed up as follows:

---

52. *Information Privacy Act 2000* (Vic) s 19(4).

53. A Bendall, “The Governance of Privacy: Speak softly and carry a big stick” (Paper presented to the 2008 Australian Institute of Administrative Law Forum, Melbourne, 8 August 2008) 12.

54. *Information Privacy Act 2009* (Qld) s 157.

55. *Statutory Instruments Act 1992* (Qld) s 49-51.

56. *Privacy and Personal Information Protection Act 1998* (NSW) s 29(7)(b).

57. See Statutory Review of PPIPA, [11.10]; Inner City Legal Centre, *Submission*, 40.

58. Cyberspace Law and Policy Centre, *Submission*, 29; Australian Privacy Foundation, *Submission to the NSW Attorney General’s Department Review of the Privacy and Personal Information Protection Act 1998* (2004) 6; Inner City Legal Centre, *Submission*, 40.

59. NSW Law Reform Commission *Privacy Principles*, Report 123 (2008) (“NSWLRC Report 123”) 4. (“Regulations” refers to all regulatory instruments, including privacy codes and PIDs.)

There is an inherent policy conflict in making codes that are to be made for the privacy protection of individuals (section 29) when they can only diminish the privacy protections in the IPPs (section 30).<sup>60</sup>

7.34 We acknowledge the concerns raised by many of the submissions from government agencies that, as matters currently stand, codes are necessary for their proper functioning. We also note that, as the Office of Industrial Relations submitted, “there would be greater benefits to agencies and the public at large, in the form of transparency and consistency, if such exemptions were self contained within the Act”.<sup>61</sup>

### *Submissions*

7.35 One of the concerns expressed in CP 3 was that the discrepancy between s 29(2) (which allows codes of practice “to regulate” personal information), and s 30(1) (which allows codes to “modify” the application of the IPPs), results in ambiguities in the precise scope of what codes of practice are able to do. It would seem that the term “regulate” would allow a code to do more than merely modify the application of IPPs. In CP 3 we asked:<sup>62</sup>

- a) Whether the interaction of s 29(2) of PPIPA with s 30(1) of that Act should be clarified?
- b) Whether the precise scope of a privacy code of practice should be clarified?

7.36 All submissions addressing these issues agreed that clarification was necessary. The main forms of clarification proposed were as follows:

- (1) Repeal the provisions. This was supported by reference to the use of s 41 directions instead of codes. It is unnecessary to have two methods for achieving the same goals.<sup>63</sup> It has also been submitted that s 41 directions “are even less transparent and accountable” than the use of codes,<sup>64</sup> and that serious

---

60. Statutory Review of PPIPA, [11.8].

61. Office of Industrial Relations, *Submission*, 1.

62. NSWLRC CP 3, Issues 48 and 49.

63. Australian Privacy Foundation, *Submission*, 12.

64. Australian Privacy Foundation, *Submission*, 12.

derogations from legislative standards should be only made by Parliament.<sup>65</sup>

- (2) Increase the accountability and transparency mechanisms in the creation and adoption of codes.<sup>66</sup> The submissions here suggested that there should be a public interest test similar to that applying to s 41 directions, and also a public consultation requirement similar to that in the *Privacy Act 1988* (Cth).<sup>67</sup>
- (3) Modify the role of codes so that they cannot derogate from the legislative standards, but only increase privacy protection, similarly to the Commonwealth provisions and the proposed UPPs.<sup>68</sup> This would mean that codes would no longer be able to “regulate” the application of privacy principles under s 29(2), and that a provision would be inserted similar to s 18BB(2)(a) of the *Privacy Act 1988* (Cth) stating that the code must set out obligations at least the equivalent of the privacy principles. This is particularly attractive given the ALRC’s recommendation for national uniformity,<sup>69</sup> which we support, and our consequent recommendation for the adoption of the suitably modified UPPs in Report 123.<sup>70</sup>

7.37 We recommend the adoption of both (2) and (3), provided that the proposed UPPs are adopted in NSW. This is because, as will be shown, what is achieved by the existing codes in practice will be covered by the UPPs, with minor exceptions. We do not recommend the removal of privacy codes, because it is important to maintain the potential for “sector-specific” interpretation; for the ability to address “new and

---

65. Australian Privacy Foundation, *Submission*, 12; Cyberspace Law and Policy Centre, *Submission*, 29.

66. Cyberspace Law and Policy Centre, *Submission*, 29.

67. Cyberspace Law and Policy Centre, *Submission*, 29. The *Privacy Act 1988* (Cth) requires the Commonwealth Privacy Commissioner to “consult any person the Commissioner considers appropriate” (s 18BB(1)) and provide members of the public the opportunity to comment on a draft of the code (s 18BB(2)(f)).

68. Inner City Legal Centre, *Submission*, 40.

69. ALRC Report 108, vol 1, [3.65]-[3.69], NSWLRC Report 123, [0.10]-[0.12], NSWLRC CP 3, Proposal 1.

70. See further NSWLRC Report 123.

developing technologies”;<sup>71</sup> and for the increasing of privacy standards where appropriate.<sup>72</sup>

### RECOMMENDATION 7.3

Privacy legislation in NSW should provide that privacy codes of practice cannot derogate from the standards prescribed in privacy legislation, but only increase privacy protection or clarify the operation of privacy principles.

### RECOMMENDATION 7.4

A public consultation requirement, similar to that in Part 3AA of the *Privacy Act 1988* (Cth), should be adopted to increase the accountability and transparency mechanisms in the creation and adoption of privacy codes.

### RECOMMENDATION 7.5

If Recommendation 7.3 is not adopted, a requirement to publish a statement of reasons in relation to the making of privacy codes, similar to s 79 of the *Privacy Act 1988* (Cth) relating to public interest determinations, should be adopted.

## Issues raised by current NSW privacy codes of practice

7.38 If our Recommendations are adopted, it is important to ensure that the current exemptions granted by the codes, where justified and necessary, are maintained. This involves an analysis of the code provisions to determine which exemptions are covered by the proposed UPPs and which remaining exemptions need to be contained in the Act. It requires consideration of the following issues:

- (1) reasonableness provisions;
- (2) consent and capacity;<sup>73</sup>
- (3) the application of the exemptions contained within the Act;<sup>74</sup>

71. ALRC Report 108, vol 1, [4.84].

72. Australian Privacy Foundation, *Submission to the NSW Attorney General's Department Review of the Privacy and Personal Information Protection Act 1998* (2004) 6.

73. See Chapter 3.



- (4) the investigation and law enforcement exemptions;<sup>75</sup>
- (5) whether codes constitute a “lawful excuse” for the purposes of secrecy provisions; and
- (6) the interpretive/modificatory role of the current codes.

7.39 Essentially, existing codes extend exemptions already contained in PPIPA, the functioning of which are either unclear (thus requiring code clarification), or not flexible enough to allow the proper exercise of certain agency functions. As with PIDs,<sup>76</sup> the majority of these issues are dealt with elsewhere in this report. In brief, the adoption of the proposed UPPs and the recommendations made elsewhere in this report will cover the exemptions specifically contained in the codes. If the UPPs are not adopted, then the legislation should be amended to encompass the exemptions provided for in the codes, either by including them in PPIPA, or by modifying the IPPs. We have made some alternative recommendations to this effect with regard to law enforcement and investigative agencies.<sup>77</sup>

---

#### RECOMMENDATION 7.6

If the UPPs are not adopted, the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to encompass the exemptions provided for in the codes of practice.

#### Reasonableness provisions

7.40 The majority of codes have reasonableness provisions relating to direct collection of personal information from individuals.<sup>78</sup> These provisions state that non-compliance with the collection principle is allowed where it is “unreasonable or impracticable” to obtain information directly from an individual, or with the consent of that individual, for example where there is a time constraint and urgent collection is

---

74. See Chapter 4 and Chapter 6.

75. See Chapter 5.

76. See para 7.66-7.91.

77. See Chapter 5.

78. See Appendix B.

required<sup>79</sup> or there is suspected fraud<sup>80</sup> by the individual, or where it would detrimentally affect or prevent the exercise of the agency's functions.<sup>81</sup> Similar code provisions exempt agencies from compliance with s 10 of PPIPA<sup>82</sup> where to do so would jeopardise an investigation or the security or safety of individuals or of facilities such as correctional centres.<sup>83</sup>

7.41 There are also a number of codes that exempt agencies from use or disclosure requirements where this is necessary for the effective delivery of necessary services. For example, the *Privacy Code of Practice (General) 2003* ("the General Code") allows, in Part 4, for human services agencies to collect, use and disclose personal information, despite the operation of the IPPs, where a senior officer has given authorisation. Authorisation can only be granted if certain criteria are satisfied – principally, where there are reasonable grounds to believe that there is a "risk of substantial adverse impact" on the individual concerned or another individual if the information is not dealt with contrary to the IPPs, and reasonable steps have been taken to notify the individual of the details of the proposed authorisation.

7.42 This appears to resemble UPP 5.1(c) where use or disclosure not for the primary purpose is allowed where:

- (c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to:
  - (i) an individual's life, health or safety; or
  - (ii) public health or public safety.

7.43 However, the code provision only requires a "risk of substantial adverse impact", which under cl 10 of the General Code "includes, but is not limited to, serious physical or mental harm, significant loss of benefits

---

79. Privacy Code of Practice for the Department of Housing, in relation to the *Priority Housing Assistance Program*. See Appendix B.

80. Privacy Code of Practice for the Department of Housing.

81. Privacy Codes of Practice for the Bureau of Crime Statistics and Research, the Department of Education and Training, the Department of Fair Trading. See Appendix B.

82. Section 10 provides that where a public sector agency collects an individual's personal information, it must notify him or her, among other things, of the fact of the collection and the purpose of the collection.

83. *Privacy Code of Practice (General) 2003* (NSW) cl14(1)(d). See Appendix B.

or other income, imprisonment, loss of housing or the loss of a carer”, which is wider than “a serious threat to an individual’s life, health or safety” and does not include clause (ii).

7.44 On its face, UPP 5.1(c) does not fully cover the code exemption, but it would when taken in conjunction with the reasonableness exemption in UPP 5.1(a), which requires that:

- (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and
- (ii) the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose and the agency has no reason to believe that the individual would object.

7.45 This is wider than the current exemptions under s 17 and s 18, which require the secondary purpose to be “directly related” to the primary purpose. It would seem that the purposes envisioned by the code provisions would be related to the primary purpose of collecting information in that context; namely, to deliver services effectively and provide help to that individual. The idea of “reasonable expectation” is to be understood in a commonsense way and is not overly onerous.<sup>84</sup> If there is no reason to believe that the individual would object, therefore, it seems that the use or disclosure contemplated by this provision would be covered under the proposed UPPs. Again, as we have emphasised, guidelines can be included in the codes to aid with interpretation and clarity.<sup>85</sup>

7.46 The proposed UPP 2.3 includes an unreasonableness exemption.<sup>86</sup> Several of the submissions we received supported the adoption of such an exemption.<sup>87</sup>

---

84. ALRC Report 108, vol 2, [25.39].

85. The ALRC has specifically anticipated that guidance will be developed to aid the interpretation of this particular UPP: ALRC Report 108, vol 2, [25.54].

86. It is in UPP 2.3, however, expressed as a leading phrase – “if it is reasonable and practicable?” – not as a rider. See NSWLRC CP 3, [6.9]-[6.17]. Other Australian jurisdictions all include a similar exemption: *Information Privacy Act 2000* (Vic) sch 1 IPP 1.4, *Personal Information Protection Act 2004* (Tas) sch 1 PIPP 1.4,

## Young people and people lacking capacity

7.47 PPIPA does not provide for consent to be given other than by the individual concerned, except for two exceptions in s 9 relating to direct collection (where the individual has authorised another, or where the individual is under 16 and their parent or guardian provides the information). The first exception still requires the individual to have the capacity to give another authorisation, while the second exception is limited in scope to young people. This obviously raises issues for people over the age of 16 who do not have the capacity either to consent or to give authorisation.<sup>88</sup>

7.48 HRIPA provides for this with a general statement about capacity.<sup>89</sup> It provides that where an individual is incapable of performing an act, an “authorised individual” can perform the act on their behalf. This is the general approach that has been taken both in the General Code with regard to ageing, disability and home care services<sup>90</sup> and in various other codes.<sup>91</sup> The need for privacy codes addressing capacity demonstrates a gap in privacy legislation. We have made recommendations to address issues relating to young people and people lacking capacity in chapter 3.

## The application of current Part 2, Division 3 exemptions

7.49 Many of the code provisions exempt particular dealings with personal information which are essentially covered by the currently existing exemptions in Part 2, Division 3. For example, the Privacy Code of Practice for the Department of Education and Training contains several provisions that directly reference respective sections of PPIPA. This may indicate that the Department was unclear about the application of these exemptions and wished to clarify their scope, or additionally, that the Department wished, for the purposes of accessibility, to include all the applicable exemptions in the code applying to them.

---

*Information Act (NT) sch 2 IPP 1.4, Health Records and Information Privacy Act 2002 (NSW) sch 1 HPP 3.*

87. Cyberspace Law and Policy Centre, *Submission*, 19-20; Privacy NSW, *Submission*, 3.

88. Cyberspace Law and Policy Centre, *Submission*, 20.

89. *Health Records and Information Privacy Act 2002 (NSW) s 7-8.*

90. *Privacy Code of Practice (General) 2003 (NSW) pt 4.* See Appendix B.

91. See, for example, the Privacy Code of Practice for the Department of Education and Training.

7.50 Several submissions to CP 3 raised concerns about the clarity of Part 2, Division 3 exemptions. We have addressed them in chapters 4 to 6.

### Investigation and law enforcement exemptions

7.51 The majority of codes have provisions exempting the investigative and complaint handling functions of agencies from various IPPs. This is because s 24 of PPIPA has only limited exemptions from compliance with certain IPPs for a small list of “investigative agencies”. These exemptions are extended to all public sector agencies or officials if they are currently “investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency”.<sup>92</sup> We have noted that this is inadequate for the proper functioning of many agencies and have addressed this point, concluding that the exemptions for “enforcement bodies” under the proposed UPPs cover these code provisions.<sup>93</sup>

### Whether codes constitute a “lawful excuse”

7.52 It is our view that codes, and indeed, PIDs,<sup>94</sup> do constitute a “lawful excuse” for the purpose of secrecy provisions.<sup>95</sup> A lawful excuse is:

a reason recognised by law as sufficient justification for such failure, whether by way of answer, defence, justification or other legal right or immunity.<sup>96</sup>

7.53 The concept of a lawful excuse is thus very broad, though dependent on the context of the legislative provision that recognises the excuse.<sup>97</sup> The word “lawful” has been held to mean “not forbidden by law”, rather than the more specific term “authorised by law”.<sup>98</sup> “Law”

---

92. *Privacy and Personal Information Protection Act* (NSW) s 24(4).

93. See para 5.43.

94. See para 7.75-7.76.

95. See eg *Children and Young Persons (Care and Protection) Act 1998* (NSW) s 254; *Community Welfare Act 1987* (NSW) s 76; *Crimes (Administration of Sentences) Act 1999* (NSW) s 76.

96. *Attorney-General (Cth) v Breckler* (1999) 197 CLR 83, 103.

97. *Wilson v McDonald* (2009) 253 ALR 560, [29], [53]-[63]; *Hancock v Birsa* [1972] WAR 177, [179].

98. *Wilson v McDonald* (2009) 253 ALR 560, [58]; *Roddan v Walker* (1997) 94 A Crim R 170, 180-181.

includes court orders,<sup>99</sup> and, under our recommendations, also “documents that are given the force of law”, which includes industrial awards.<sup>100</sup> It appears that conduct contemplated by a code would be conduct for which there is a “lawful excuse”. A similar argument applies for PIDs.<sup>101</sup>

### The interpretive role of the current codes

7.54 The majority of the presently existing codes of practice, even where they derogate from the IPPs, provide a level of privacy protection that is, overall, equal to that contained in the proposed UPPs. This is achieved through fairly detailed procedural guidelines as to the situations in which derogation from the IPPs is permitted, and how personal information will be dealt with in these situations. For example, the Privacy Code of Practice for the NSW Public Sector Workforce Profile is potentially the most invasive of all the codes, dealing as it does with the personal information not only of all public sector employees but also of private contractors.<sup>102</sup> Yet it provides a list of the types of information collected and processed;<sup>103</sup> procedures for dealing with the personal information, involving notification and where possible the gaining of informed consent;<sup>104</sup> the exact purposes to which the information will be put;<sup>105</sup> a method of complaints-handling and review; and a companion to the provisions of the code outlining further responsibilities and procedures.<sup>106</sup>

7.55 Similarly, the Privacy Code of Practice for the Department of Fair Trading outlines the purposes of and reasons for the code; how it relates to the functions of NSW Fair Trading, and in what circumstances the exemptions will be invoked.

---

99. *Re An Application by the NSW Bar Association* [2004] FMCA 52; *GV v Office of the Director of Public Prosecutions* [2003] NSWADT 177.

100. See para 4.26-4.31 (in relation to non-compliance where “required or authorised by law”); ALRC Report 108, vol 1, Recommendation 16-1.

101. See para 7.75-7.76.

102. Privacy Code of Practice for the NSW Public Sector Workforce Profile, pt 1, [1]. See Appendix B.

103. Privacy Code of Practice for the NSW Public Sector Workforce Profile, pt 1, [4].

104. See generally, Privacy Code of Practice for the NSW Public Sector Workforce Profile, pt 1, [6].

105. Privacy Code of Practice for the NSW Public Sector Workforce Profile, pt 1, [5].

106. Privacy Code of Practice for the NSW Public Sector Workforce Profile, pt 2.

7.56 Although the level of detail, interpretation and justification contained in the codes is generally unobjectionable, there are some concerns as to the extent of certain exemptions granted by the codes. For example, the Privacy Code of Practice for Local Government exempts Councils from s18 where disclosure is to another agency that has approached the Council in writing, and where the Council is satisfied that the personal information is to be used for the lawful and proper functions of that agency and is reasonably necessary to do so. The generality of the phrase “lawful and proper functions” could allow information to be gathered from Councils almost at large, bypassing the collection and notification principles.

### The Commission’s view

7.57 Our approach is based on the view that the UPPs, recommended in Report 123, should act as a baseline minimum. This will provide the benefits of national uniformity and consistency, reduced complexity, and increased transparency and efficiency. The proposed UPPs are suited to this role as they are broader and more flexible than the IPPs, and are meant to act as high-level principles that are fleshed out by more specific instruments and guidelines.<sup>107</sup>

7.58 The adoption of suitably modified UPPs, as we have recommended,<sup>108</sup> will rectify the issues relating to the reasonableness provisions contained in codes. Seven of the 11 proposed UPPs contain reasonableness provisions.<sup>109</sup> What is “reasonable” is determined by what a reasonable person would consider appropriate in the circumstances.<sup>110</sup> The majority of these code provisions invoke the criterion of effective departmental function in relation to the delivering of essential human services.<sup>111</sup> It is clear that these cases are those envisaged by the reasonableness provisions, but careful guidelines and procedures need to be put in place to limit abuse.

---

107. See ALRC Report 108, vol 1, ch 4, especially [4.38]-[4.61]; NSWLRC Report 123; and para 7.3.

108. NSWLRC Report 123.

109. UPPs 1, 2, 3, 5, 7, 8, 9.

110. NSWLRC Report 123, Recommendation 2.

111. See, for example, the Privacy Code of Practice for the Department of Education and Training, and the *Privacy Code of Practice (General) 2003* (NSW) provisions relating to human and corrective services, Appendix B.

7.59 The reasonableness provisions are also aimed at facilitating effective dealing with personal information for investigative, complaints handling or law enforcement functions.<sup>112</sup>

7.60 As we have noted above, privacy codes of practice do have a role to play in modifying or interpreting the role of privacy principles to meet sector-specific needs and practices, as evidenced, for example, by the ageing, disability and home care services section of the General Code.<sup>113</sup> The Department-specific codes of practices generally maintain a level of privacy protection that would be equivalent to that which is provided for by the UPPs, and in addition, set out detailed guidelines and procedures for the application of the privacy principles. Some even include additional provisions that go beyond what is included in the current IPPs. This is to be commended. For example, the Privacy Code of Practice for the Department of Housing makes unsolicited information subject to the use, storage and access provisions of the Act.<sup>114</sup>

7.61 We thus recommend the retention of privacy codes, if they do not derogate from the UPPs and provide a level of privacy protection “overall, at least the equivalent of” the legislative standards in the Commonwealth provisions. We agree with the ALRC’s view that privacy codes should not replace, but rather operate in addition to, and provide guidance on, the application of the privacy principles.<sup>115</sup> Additionally, we recommended a level of public consultation in the adoption of codes in order to increase transparency and accountability<sup>116</sup>.

7.62 We also recommend, in line with the proposed Commonwealth model, that codes should be made by the Privacy Commissioner, not by the Minister. If our recommendations in Report 125 are adopted, the Privacy Commissioner will have to make codes with the approval of the Information Commissioner.<sup>117</sup> We have recommended that the Joint Committee<sup>118</sup> should be responsible for oversight of the Privacy

---

112. See para 5.23.

113. See Appendix B and para 7.48.

114. Privacy Code of Practice for the Department of Housing. See Appendix B.

115. ALRC Report 108, vol 2, Recommendation 48-1.

116. See Recommendation 7.4.

117. See NSWLRC Report 125, Recommendation 12.

118. See *Government Information (Information Commissioner) Act 2009* (NSW) s 44. “Joint Committee” means the Committee on the Office of the Ombudsman and the Police Integrity Commission constituted under the *Ombudsman Act 1974*



Commissioner's functions as well of those of the Information Commissioner.<sup>119</sup> This will help ensure that the Commissioners are exercising their power appropriately. If the recommendations in Report 125 are not adopted, the Privacy Commissioner should not require approval from the Information Commissioner.

7.63 We note that derogation from legislative standards, according to our recommendations below and following the ALRC's regulatory model,<sup>120</sup> can be achieved temporarily through the use of PIDs or permanently through regulation.<sup>121</sup>

---

#### RECOMMENDATION 7.7

If Recommendation 12 of Report 125 is adopted, the creation and amendment of privacy codes of practice should be performed by the Privacy Commissioner with the approval of the Information Commissioner.

---

#### RECOMMENDATION 7.8

If Recommendation 12 of Report 125 is not adopted, the Privacy Commissioner should make and amend privacy codes of practice.

#### *If the UPPs are not adopted*

7.64 If it is deemed inadvisable to remove the ability of privacy codes to derogate from legislative standards, for example, if the proposed UPPs are not adopted, we still recommend that their creation, modification, and use be much more closely monitored. This would involve a public consultation requirement, public interest test and the requirement to give reasons.

7.65 If the UPPs are not adopted, our alternative recommendations relating to specific exemptions and law enforcement and investigative bodies<sup>122</sup> will cover the exemptions given in the codes. This would mean

---

(NSW) or such other joint committee of members of Parliament as may be appointed to exercise the functions of the Joint Committee under the *Government Information (Information Commissioner) Act 2009* (NSW): s 3.

119. NSWLRC Report 125, Recommendation 16.

120. ALRC Report 108, vol 1, ch 4.

121. See Recommendations 7.1, 7.12.

122. See Recommendations 5.2-5.3.

that the codes, in reference to these points, would only clarify and provide guidance on where the PPIPA exemptions apply. To the extent that the code provisions are not covered by our recommendations, we recommend that they are included in the Act, either as specific exemptions or as exemptions to the IPPs.

## PUBLIC INTEREST DIRECTIONS

7.66 PIDs are covered under s 41 of PPIPA (and s 62 of HRIPA), which allows the Privacy Commissioner, with the approval of the Minister, to make a written direction indicating that an agency (or in the case of HRIPA, an “organisation”)<sup>123</sup> is not required to comply with an IPP or code or that the application of an IPP or code is modified for that agency.<sup>124</sup> This direction should only be made where the Privacy Commissioner is satisfied that the public interest in requiring the agency to comply with the principle or a code is outweighed by the public interest in the Privacy Commissioner making the direction.<sup>125</sup>

7.67 The Privacy NSW website notes that PIDs are only intended to apply temporarily until an appropriate code of practice is developed. The process of applying the public interest test may involve consultation with parties that are affected by the direction and the Commissioner may ask the agency for reasons and further information.<sup>126</sup>

7.68 However, out of the 11 PIDs currently in place, eight have been in place for over six years, and the remaining three have unspecified end dates.<sup>127</sup> These three are, however, all “pilot” or “trial” programs.

7.69 This confirms the observations made above with respect to privacy codes, namely that there exist significant practical shortcomings with the current system and that, similarly to privacy codes, the use of PIDs has

---

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

124. *Privacy and Personal Information Protection Act 1998* (NSW) s 41(1).

125. *Privacy and Personal Information Protection Act 1998* (NSW) s 41(3).

126. Privacy NSW, “Public Interest Directions: How is a public interest direction made?”, <[http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_03\\_ppips4](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_ppips4)> at 1 October 2009.

127. See Appendix C.

been “stretched”<sup>128</sup> to allow agencies to function properly. As the Statutory Review of PPIPA put it:

The main problem with the use of section 41 directions is that what should be a short-term solution to an information management problem becomes the effective long-term solution. The directions are simply re-made continuously as they expire because of lack of satisfactory progress on negotiating a more long-term solution.<sup>129</sup>

7.70 We are of the view that a statutory basis for long-term exemptions is vastly preferable to the use of PIDs, and that the use of PIDs should be limited to the original intent behind the provisions – as temporary measures. The following analysis will identify both general issues raised by several PIDs, and, where appropriate, deal with issues raised by specific PIDs. For information specific to a particular direction, we have included a table in the Appendix C.

## Issues

7.71 The general issues that are raised by the PIDs fall into two categories: issues raised by the content of PIDs, which are substantially similar to those raised by codes, and issues to do with the role of PIDs. The issues addressed by the content are as follows:

- (1) capacity and consent;<sup>130</sup>
- (2) the application of the specific exemptions;<sup>131</sup> and
- (3) research exemptions.

The first two of these have been dealt with elsewhere in this report.<sup>132</sup>

7.72 The issues associated with the role of PIDs generally are:

- (1) whether PIDs constitute a “lawful excuse”;
- (2) temporary PIDs – trial or pilot projects;

---

128. Australian Privacy Foundation, *Submission*, 13.

129. Statutory Review of PPIPA, [11.16].

130. See Appendix C, “Direction relating to The Department of Ageing, Disability and HomeCare and Associated Agencies” and Chapter 3.

131. See Appendix C generally.

132. For consent and capacity, see Chapter 3; for the specific exemptions see Chapters 4-6.

- (3) the lack of consultation requirements;
- (4) whether PIDs should apply to classes of agencies; and
- (5) whether PIDs should be able to be amended.

### *Research Exemptions*

7.73 The “Direction Relating to the Disclosures of Information by NSW Public Sector Agencies for Research Purposes” exempts agencies from compliance with collection, notification, alteration, use and disclosure IPPs where reasonable departure is necessary for research purposes.

7.74 Proposed UPPs 2.5(f), 5.1(g) and 9.6 now cover this Direction and make it unnecessary. In the event that the proposed UPPs are not adopted, we recommend that this Direction be incorporated into the Act. This would also cover the “Direction on Disclosures of Information by the New South Wales Public Sector to the National Coronial Information System (NCIS)”.

## RECOMMENDATION 7.9

If the UPPs are not adopted, the “Direction Relating to the Disclosures of Information by NSW Public Sector Agencies for Research Purposes” should be incorporated as a specific exemption to the collection, notification, use and disclosure IPPs.

### *Whether PIDs constitute a “lawful excuse”*

7.75 As discussed above with regard to privacy codes of practice,<sup>133</sup> it is our view that PIDs, depending on the terms of the direction,<sup>134</sup> will constitute a lawful excuse for the purpose of secrecy provisions. This position accords with our proposed definition of “law” (for the purposes of the “required or authorised by law” exception to the privacy principles), which would include PIDs.<sup>135</sup> Our recommendation to make PIDs disallowable by Parliament will also support PIDs constituting a “lawful excuse”.<sup>136</sup>

133. See para 7.52-7.53.

134. See *Privacy Act 1988* (Cth) s 72(5).

135. See para 4.26-4.31.

136. See para 7.90; Recommendation 7.12(5).

7.76 If it is still felt to be unclear whether or not PIDs constitute a lawful excuse, provision should be made in the legislation to confirm that they do. This could take the form of a direct provision stating that PIDs constitute a lawful excuse or by modifying the statutory language such that PIDs act to “authorise” conduct, perhaps by modifying s 41(2).

*Temporary PIDs – trial or pilot projects*

7.77 The second general issue that is raised by the PIDs is the status of trial and pilot projects. The exemptions granted by the long standing PIDs are all covered by the proposed UPPs, particularly by the introduction of the reasonableness provisos. However, we acknowledge and emphasise that, given the high-level generality of the UPPs, there is much room and need for the development and application of guidelines and codes in order to clarify agencies’ obligations. In order to be clear, we do believe that the exemptions currently included in the PIDs are all similarly included in the proposed UPPs.

7.78 We accept that the role of PIDs should be to function temporarily in situations where immediate flexibility is required. The prime example of this is in the case of a trial or pilot project involving multiple agencies where it is unclear exactly what powers are required for the proper functioning of the project. In these circumstances, it may be appropriate for exemptions from certain privacy principles to apply. However, we urge that these exemptions must still be subject to the basic requirements of openness and accountability,<sup>137</sup> and that they should not extend beyond what is prima facie necessary for the operation of a project.

7.79 The recently revoked “Direction Relating to the Document Verification Service, NSW Registry of Births, Deaths and Marriages” is a good example of this.<sup>138</sup> This PID was passed on the 9 July 2009 and was valid for six months. It exempted the NSW Registry of Births, Deaths and Marriages from compliance with s 9, s 10, s 11, s 17 and s 18 where personal information would be collected, used or disclosed for the purposes of the Document Verification Service (“DVS”), which verifies the accuracy of proof of identity (“POI”) documents. The Registry in relation to the DVS is now covered by a section of the General Code.<sup>139</sup>

---

137. See para 7.81-7.82.

138. Although this direction is no longer in force, we include it in the table in the appendix for reference purposes.

139. See Appendices B and C.

7.80 The DVS requires the consent of the person for the verification of their POI documents. The PID was passed only in order to ascertain exactly what exemptions were necessary for the operation of the DVS, which as of 30 December 2009 is covered by the General Code. This relationship between the temporary use of a PID and the longer-term use of a code or a regulation is precisely what is envisaged by the legislation.

*The lack of consultation requirements*

7.81 Several submissions raised the issue of the transparency of PIDs.<sup>140</sup> The Statutory Review of PPIPA also raised this concern.<sup>141</sup> As outlined above, the making of PIDs does not *require* public consultation, although the process may involve consultation with affected parties.

7.82 The Commonwealth public interest determination provisions require that the public interest in favour of the determination “substantially outweighs” the public interest in adhering to the privacy principles.<sup>142</sup> The Commonwealth Privacy Commissioner must prepare a draft determination and invite submissions on it.<sup>143</sup> The Commissioner is required to take these submissions into account,<sup>144</sup> must keep a register of determinations<sup>145</sup> and is required to give a statement of reasons for the determination.<sup>146</sup> The determination is also a disallowable instrument.<sup>147</sup> It was submitted that this would be a good model for PPIPA to adopt.<sup>148</sup> It has the benefits of increasing openness and providing legislative criteria by which the process of making a PID can be adjudged. However, given that PIDs are meant to be temporary instruments, a full-blown public consultation process may make the creation process unworkably lengthy.

*Classes of agencies*

7.83 In CP 3, we raised the issue of whether PIDs should be able to apply to a class of agencies. If PIDs are to play the temporary role we envisage, we believe that there is no compelling reason why PIDs should

---

140. See eg Cyberspace Law and Policy Centre, *Submission*, 30; Australian Privacy Foundation, *Submission*, 13.

141. Statutory Review of PPIPA, [11.13]-[11.23].

142. *Privacy Act 1988* (Cth) s 72(2)(b).

143. *Privacy Act 1988* (Cth) s 75.

144. *Privacy Act 1988* (Cth) s 79(2).

145. *Privacy Act 1988* (Cth) s 80E.

146. *Privacy Act 1988* (Cth) s 79(3).

147. *Privacy Act 1988* (Cth) s 80(1).

148. Cyberspace Law and Policy Centre, *Submission*, 30.

not be able to apply to a class of agencies. The submissions were generally in agreement on this point.<sup>149</sup> We note, however, that the argument was made that the public should know exactly which agencies are subject to exemptions.<sup>150</sup>

#### RECOMMENDATION 7.10

Section 41 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to allow the Privacy Commissioner to make a public interest direction that applies to a class of agency.

#### *The amendment of PIDs*

7.84 We also raised the issue in CP 3 of whether PIDs should be subject to amendment.<sup>151</sup> All submissions that responded to this issue were in agreement on this<sup>152</sup> and we see no reason why s 41 should not be changed to allow PIDs to be amended, of course subject to the public consultation process and requirement to give reasons.<sup>153</sup> The amendment process would be the same as the creation process, except of course that submissions and the statement of reasons need only refer to the proposed amendment. It should be made clear that the amendment of a PID does not extend the time that it is effective.

#### RECOMMENDATION 7.11

Section 41 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to give the Privacy Commissioner the power to amend an earlier public interest direction.

#### The Commission's view

7.85 We believe that the same issues are present in relation to PIDs as in relation to privacy codes. More specifically, PIDs address the difficulties that certain agencies and programs have in functioning effectively and

149. Australian Privacy Foundation, *Submission*, 13; Cyberspace Law and Policy Centre, *Submission*, 30.

150. Inner City Legal Centre, *Submission*, 40.

151. NSWLRC CP 3, Proposal 17.

152. Australian Privacy Foundation, *Submission*, 13; Cyberspace Law and Policy Centre, *Submission*, 30; Inner City Legal Centre, *Submission*, 18.

153. See Recommendation 7.12.

properly where consent is required for the collection or disclosure of certain information. The relaxation of the collection and use or disclosure requirements in the proposed UPPs, or, rather, the clarification, codification and increased flexibility of their exceptions, would make redundant the existing long standing PIDs.

7.86 While most of the aims of the existing short-term PIDs will be achieved by the adoption of the UPPs, we recognise that it may be desirable for the sake of certainty for agencies to have specific exemptions apply for trial projects. However, if this is to be the case, then the process should have greater transparency than at present.

7.87 Under s 41, the Privacy Commissioner must be satisfied that the balance of the public interest favours the making of the PID. This decision is made without the benefit of public consultation,<sup>154</sup> and, unlike the *Privacy Act 1988* (Cth), there is no requirement for reasons to be given.<sup>155</sup> The adoption of these requirements will improve transparency and accountability, and will also contribute to a “culture of voluntary compliance with the law”.<sup>156</sup> We recognise that there may be a concern that this would “potentially reduce the flexibility of the Act and its ability to respond quickly to emerging and unforeseen projects and developments”.<sup>157</sup> However, the primary object of the legislation is to “promote the protection of the privacy of individuals”.<sup>158</sup> Any method by which this could be rolled back should therefore be subject to stringent controls. Indeed, the Statutory Review of PPIPA argued for the complete abolition of PIDs in favour of the regulation-making power.<sup>159</sup>

7.88 We therefore recommend the adoption of provisions that require public consultation for PIDs that apply for more than 12 months or

---

154. Cyberspace Law and Policy Centre, *Submission*, 30. The *Privacy Act 1988* (Cth) pt 6 div 1 requires consultation and the taking of submissions.

155. *Privacy Act 1988* (Cth) s 79(3).

156. Australian Transactions Reports and Analysis Centre, AUSTRAC Supervisory Framework <[www.austrac.gov.au/files/supervisory\\_framework.pdf](http://www.austrac.gov.au/files/supervisory_framework.pdf)>, accessed on 2 Feb 2010, quoted in ALRC Report 108, vol 1, [4.17].

157. NSW Government Response to the Statutory Review, 10.

158. NSW, *Parliamentary Debates*, Legislative Council, 17 September 1998, 7599 (Hon J Shaw, Attorney General).

159. Statutory Review of PPIPA, Recommendation 21.



require renewal.<sup>160</sup> We further recommend a requirement that the Privacy Commissioner publish a statement of reasons for a PID. Additionally, we recommend that there is a final limit of the length of a PID to 3 years, including renewals, unless the Privacy Commissioner decides that there are exceptional circumstances that warrant a further extension. This provides the flexibility needed in exceptional circumstances while recognising that PIDs are only meant to be temporary instruments and not final solutions. For example, a research project may require exemptions for longer than 3 years, or it may be unclear after 3 years whether a particular project is worth continuing. Factors such as these will have to be taken into account by the Privacy Commissioner.

7.89 For the sake of uniformity,<sup>161</sup> provisions similar to the Commonwealth provisions should be introduced, including the requirement that the public interest in favour of the determination “substantially outweighs” the public interest in adhering to the privacy principles. While transparency and accountability are required, we do recognise that PIDs are meant to be temporary measures while longer term solutions are being crafted. Speed and flexibility are thus more important with PIDs than with the crafting of codes or regulations.

7.90 We also recommend that PIDs that require consultation should be disallowable by Parliament. This is consistent with the approach taken by Commonwealth privacy legislation.<sup>162</sup> This does not require that PIDs are “statutory rules” for the purposes of the *Subordinate Legislation Act 1989* (NSW).<sup>163</sup> The Privacy Commissioner should also be required to ensure that all PIDs are publicly available.<sup>164</sup>

7.91 As with privacy codes, we believe that the Privacy Commissioner should be able to create and amend PIDs without the approval of the

---

160. Australian Privacy Foundation, *Submission*, 13; Statutory Review of PPIPA, [11.18].

161. ALRC Report 108, [3.109].

162. *Privacy Act 1988* (Cth) s 80, s 80C. See also ALRC Report 108, [3.109].

163. C J Boulton (ed), *Erskine May's Treatise on the Law, Privileges, Proceedings and Usage of Parliament* (21<sup>st</sup> ed, 1989) 540, 542.

164. We note that the Privacy Commissioner currently publishes PIDs on their website. We simply wish to ensure that this practice continues. The Commonwealth Privacy Commissioner must keep a public register of all public interest determinations: *Privacy Act 1988* (Cth) s 80E.

Minister.<sup>165</sup> This approach is consistent with the *Privacy Act 1988* (Cth).<sup>166</sup> If Recommendation 12 of Report 125 is adopted, the Information Commissioner will be responsible for approving PIDs.<sup>167</sup>

#### RECOMMENDATION 7.12

---

In relation to public interest directions, s 41 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include:

- (1) A requirement that the public interest in favour of the public interest direction “substantially outweighs” the public interest in adhering to the privacy principles.
- (2) A limit on the duration of a public interest direction to 12 months without consultation, and a final limit of 3 years (including renewals) unless the Privacy Commissioner decides there are exceptional circumstances that warrant extending or renewing the public interest direction.
- (3) A requirement that the Privacy Commissioner, before issuing a public interest direction of a duration longer than 12 months or renewing a direction, accept public submissions and take these submissions into account.
- (4) A requirement that the Privacy Commissioner publish a statement of reasons for any public interest direction.
- (5) That a public interest direction of duration longer than 12 months is a disallowable instrument.

#### RECOMMENDATION 7.13

---

The Privacy Commissioner must ensure that all public interest directions are made publicly available.

#### RECOMMENDATION 7.14

---

The creation and amendment of public interest directions should not require the approval of the Minister.

---

165. See para 7.62.

166. See *Privacy Act 1988* (Cth) s 72.

167. See NSWLRC Report 125.

## 8. **Public registers**

- Introduction
- Definition of a “public register”
- Regulation of information contained in public registers
- Issues raised by the public register provisions
- Public register regulation in other jurisdictions
- Possible methods of public register regulation

## INTRODUCTION

8.1 Public registers, because they store large amounts of personal information and are required to be publicly available, pose a particular problem for privacy. Part 6 of the *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”) implicitly recognises that although information may be publicly available, it does not for that reason cease completely to be personal or private information.<sup>1</sup> Privacy NSW has noted that:

Privacy only covers information which is personal. It emphasises concepts of fair and legal collection, up front notification and fair use, regulated by the purpose of collection. The fact that information is in the public domain will not necessarily exclude it from protection when it is collected and used for other purposes.<sup>2</sup>

8.2 The purpose of the regulation of public registers is to ensure that only the necessary amount of personal information is made public and manage the handling of this personal information. It recognises that while there are valid reasons for making certain information public (such as openness, accountability and efficiency), the information that we give to agencies and organisations should only be used for the purposes for which we have given it. In this regard, the Office of the Commonwealth Privacy Commissioner has said that:

the law should, unless there is a very strong public interest reason, restrict the collection from, and use of, personal information on a public register to the public purpose for which the register is set up and for which the information is made public. This is because generally speaking individuals have no choice about whether to provide the information and little choice about its publication.<sup>3</sup>

## DEFINITION OF A “PUBLIC REGISTER”

8.3 Part 6 of PPIPA sets out certain requirements for dealing with personal information contained in public registers. A public register is defined as “a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or

- 
1. See *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(b).
  2. Privacy NSW, “Local Government and the *Privacy and Personal Information Protection Act*”, Issues Paper (2000) pt 5.
  3. Office of the Privacy Commissioner, Consultation Paper for Information Sheet, *Privacy and Collection of Publicly Available Personal Information* (2002) [23].

not on payment of a fee”).<sup>4</sup> This would include registers not held or maintained by public sector agencies.<sup>5</sup>

8.4 We first note that there is a crossover between the exemption for information contained in “publicly available publications”<sup>6</sup> and the definition of a public register, such that if a public register is published, it may not fall within the definition of personal information.<sup>7</sup> This is reinforced by the decision in *EG v Commissioner of Police*, where it was confirmed that “publicly available publication” is to be interpreted according to its ordinary meaning as “any publication that is open to or accessible by the public by means of payment or otherwise”.<sup>8</sup> This means that Part 6 likely operates instead of, not in addition to, the Information Protection Principles (“IPPs”) as information contained in public registers. This is because “publicly available” information is not subject to the IPPs.<sup>9</sup> This is consonant with the *Information Privacy Act 2000* (Vic), which defines information on a public register as information that “would be personal information if the document were not a generally available publication”.<sup>10</sup>

8.5 It is, however, arguable that the publication – that is, the disclosure – of the information by putting it on the public register would be subject to the privacy principles, as prior to that publication it is not “publicly available”.<sup>11</sup> The Australian Privacy Foundation has noted this issue and submitted that it should be clarified.<sup>12</sup> Generally, however, the publication of information on a public register will be the primary

---

4. *Privacy and Personal Information Protection Act 1998* (NSW) s 3.

5. Compare the *Information Privacy Act 2000* (Vic) s 3, which defines a public register as “... a document held by a public sector agency”.

6. *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(b).

7. Australian Privacy Foundation, *Submission to the NSW Attorney General’s Department Review of the Privacy and Personal Information Protection Act 1998* (2004) 11.

8. *EG v Commissioner of Police* [2004] NSWADTAP 10, [46].

9. See also NSW Law Reform Commission, *Access to Personal Information*, Report 126 (2010) (“NSWLRC Report 126”) [2.52]-[2.61].

10. *Information Privacy Act 2000* (Vic) s 3(b).

11. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 92-93.

12. Australian Privacy Foundation, *Submission to the NSW Attorney General’s Department Review of the Privacy and Personal Information Protection Act 1998* (2004) 11.

purpose of the collection of that information. It is reasonable that individuals whose personal information is collected for the purposes of publication in a public register should be informed of this purpose of the collection.<sup>13</sup>

8.6 The publication would also, under the proposed Unified Privacy Principles (“UPPs”), be “required or authorised by law” as the establishing statutes for public registers generally require the information on the register to be made publicly available.<sup>14</sup>

8.7 The definition of a “public register” is thus an important issue. We have recommended that the “publicly available publication” exception to the definition of personal information under s 4(3)(b) should be repealed, and that the definition of a “record” should exclude “generally available publications”.<sup>15</sup> A public register, for the reasons above, would also likely be a “generally available publication”.<sup>16</sup> Personal information collected for or held in a generally available publication will be subject to fewer privacy principles than information held in a record.<sup>17</sup> If, as we recommend,<sup>18</sup> all of the UPPs apply to public registers, then public registers must be excluded from the definition of “generally available publication”, either specifically in the legislation or by regulation.<sup>19</sup>

---

13. See UPP 3 – Notification.

14. See, for example, the Register of Chiropractors for NSW kept under the *Chiropractors Act 2001* (NSW) sch 1 cl 21(3) which states that:

The Register must be available for inspection by any person:

- (a) in person at the office of the office of the Board at all reasonable times, and
- (b) by other such means (such as Internet access) and at such other times as the Board determines.

Similar provisions apply for the other health practitioner registers. Note that s 59, stating that the provisions of Part 6 prevail over the provisions of the Act under which the register is created, still operates to the exclusion of these provisions. See below at para 8.12.

15. NSWLRC Report 126, Recommendations 6 and 9; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”) [11.29]-[11.31].

16. ALRC Report 108, [11.33].

17. NSWLRC Report 126, [2.52]-[2.61].

18. See para 8.37-8.44, Recommendation 8.3.

19. See NSWLRC Report 126, Recommendation 6.

8.8 The current definition does not require that the register be made pursuant to an enactment. Since PPIPA only applies to public sector agencies, a public register should be defined as a register held by a public sector agency pursuant to an enactment.<sup>20</sup> This would be consistent with the ambit of PPIPA and clarify the issue of determining whether or not a particular record falls under the definition of a “public register”.<sup>21</sup> This recommendation relies on the assumption that public registers held by organisations other than State public sector agencies will be regulated by Commonwealth privacy legislation.<sup>22</sup>

#### RECOMMENDATION 8.1

If Recommendation 6 of Report 126 is adopted, public registers should be excluded from the proposed definition of “generally available publication”.

#### RECOMMENDATION 8.2

The definition of “public register” in the *Privacy and Personal Information Protection Act 1998* (NSW) should refer only to registers held by public sector agencies pursuant to an enactment.

## REGULATION OF INFORMATION CONTAINED IN PUBLIC REGISTERS

8.9 Section 57 of PPIPA requires that before disclosing personal information held in a public register the agency must be satisfied that “it is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept”. Agencies can thus require a person applying to inspect a public register to provide a statutory declaration of purpose. It has been noted, however, that the majority of registers do not have a statement of purpose in their establishing Acts or otherwise.<sup>23</sup> The

20. The *Information Privacy Act 2000* (Vic) s3 defines a public register as “a document held by a public sector agency or a Council...by force of a provision made by or under an Act”.

21. For example, rates records held by Councils may or may not be a “public register” depending on the form in which they are kept: Department of Local Government, *Is Council’s Rates Record a ‘public register’?* Circular 00/75 (2000) 2-3.

22. See ALRC Report 108, [11.33]-[11.38], [11.53]-[11.60].

23. Privacy NSW, *Local Government and the Privacy and Personal Information Protection Act*, Issues Paper (2000) pt 5. See also New Zealand, Law Commission, *Public Registers: Review of the Law of Privacy Stage 2*, Report 101 (2008) (“NZLC Report

“purpose of the register or the Act under which the register is kept” needs therefore to be gleaned from the public interests that the register serves.<sup>24</sup>

8.10 As discussed above, there are a number of exemptions to Part 6 created by regulation or code. The *Privacy and Personal Information Protection Regulation 2005* (NSW) exempts the Registrar-General from compliance with Part 6 in respect of the Torrens Title Register, the General Register of Deeds and the Central Register of Restrictions, both under the *Conveyancing Act 1919* (NSW). It also creates exemptions in favour of the Register of Land Values, the register of Justices of the Peace, the Water Access Licence Register and the register of professional political lobbyists. Part 3 of the General Code exempts various registers relating to the environment and health professionals.<sup>25</sup> The Privacy Code of Practice for Local Government partially exempts councils from the operation of s 57 insofar as a council may allow a person to inspect a public register in council premises and copy a single entry or page of the register without the council having to be satisfied of the validity of their purpose.<sup>26</sup> This code of practice also provides guidance on the phrase “purpose of the register or the Act under which the register is kept” and on the type of information that can be disclosed in bulk.

8.11 Section 58 allows for the suppression of personal information from public registers at the request of the individual. Where the safety or well-being of an individual would be affected by not suppressing the information, the agency must suppress the information unless the public interest in that information outweighs the interest of the individual.

---

101”) [1.26]; B Whiteman, “Local Government and the NZ Public Register Privacy Principles” (1994) 1 *Privacy Law and Policy Reporter* 106, section entitled “Purpose Issues”; J Edwards, “Public Registers: NZ’s approach”, (1994) 1 *Privacy Law and Policy Reporter* 85; Office of the Victorian Privacy Commissioner, *Public Registers and Privacy: Building Permit Data* (2002) [17]-[18], [26]-[28].

24. Office of the Victorian Privacy Commissioner, *Public Registers and Privacy: Building Permit Data* (2002) [28].

25. The registers excluded are registers of doctors, nurses, chiropractors, dentists, dental technicians, midwives, optometrists, osteopaths, pharmacists, physiotherapists, podiatrists and psychologists, as well as registers maintained by the Environmental Protection Authority relating to the reporting of environmental offences.

26. Privacy Code of Practice for Local Government (2000) 4. See Appendix B.



8.12 Section 59 provides that in the case of inconsistency with a public register’s enabling Act, the provisions of Part 6 prevail.

## ISSUES RAISED BY THE PUBLIC REGISTER PROVISIONS

8.13 The main issue raised by the public register provisions is the complicated method of regulation. As outlined above, the definition of a “public register” is such that it is at best unclear whether the IPPs in Part 2, Division 1 apply. Further, because of the operation of s 59 of PPIPA, public registers, unless exempted from the operation of Part 6, cannot be regulated by their parent Acts.<sup>27</sup> This creates a regime where public registers are not subject to the IPPs but may be subject to regulation from various sources. Additionally, the total exemption of certain public registers through regulation or code is unnecessary and potentially dangerous.<sup>28</sup>

8.14 The Privacy Commissioner has expressed concern that widespread circulation of public registers, for example on the internet, without controls, may allow the home address of a doctor to be made widely known to those with no legitimate right to know.<sup>29</sup>

8.15 This is exacerbated by the fact that a blanket exemption would allow health information and sensitive information potentially to be included in a public register.

8.16 The exemption of certain public registers by regulation or code is an abrogation of legislative standards that should not occur without proper consultation and accountability measures. The Australian Privacy Foundation, in its submission to the Statutory Review of PPIPA, noted that the exemption of various public registers (such as the Torrens register) by the 2000 Regulation (now the *Privacy and Personal Information Protection Regulation 2005*) occurred without “public consultation or publicly available justification”.<sup>30</sup> We note that our recommendations

---

27. NSW Attorney General’s Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly). (“Statutory Review of PPIPA”) [12.9].

28. Statutory Review of PPIPA, [12.5].

29. Statutory Review of PPIPA, [12.5].

30. Australian Privacy Foundation, *Submission to the NSW Attorney General’s Department Review of the Privacy and Personal Information Protection Act 1998* (2004) 12. Public registers maintained by local councils raise particular issues. In

regarding codes, public interest directions (“PIDs”) and regulations require public consultation and justification for proposed exemptions.<sup>31</sup>

## PUBLIC REGISTER REGULATION IN OTHER JURISDICTIONS

8.17 Other methods of regulating public registers are in effect in Victoria, New Zealand<sup>32</sup> and at the Commonwealth level. We examine these in turn.

### Victoria

8.18 Sub-section 16(4) of the *Information Privacy Act 2000* (Vic) requires that:

A public sector agency or a Council must, in administering a public register, so far as is reasonably practicable not do an act or engage in a practice that would contravene an Information Privacy Principle in respect of information collected, held, managed, used, disclosed or transferred by it in connection with the administration of the public register if that information were personal information.

---

CP 3, we invited submissions on the issue of the interrelationship between the *Privacy and Personal Information Protection Act 1998* (NSW), the *Freedom of Information Act 1989* (NSW), and the *Local Government Act 1993* (NSW). Particularly problematic was the co-regulation of council-maintained public registers by the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Local Government Act*. These issues have now largely been resolved by the passing of the *Government Information (Public Access) Act 2009* (NSW) (the “GIPA Act”). The information contained in many council-maintained public registers is deemed “open access information” under the GIPA Act. “Open access information” must be made publicly available unless there is an overriding public interest against disclosure of the information. These provisions prevail over the *Privacy and Personal Information Protection Act 1998* (NSW) by means of s 11 the GIPA Act; *Government Information (Public Access) Act 2009* (NSW) sch 5 cl 3. These GIPA provisions replace those of the *Local Government Act 1993* (NSW), which have been repealed by the *Government Information (Public Access) (Consequential Amendments and Repeal) Act 2009* (NSW); *Government Information (Public Access) Act 2009* (NSW) s 6(1). GIPA will thus clarify the duties of councils in relation to public registers, replacing the current scheme of council-maintained public register regulation that is contained in the Privacy Code of Practice for Local Government. See Appendix B.

31. See Recommendations 7.2, 7.4, 7.5 and 7.12.

32. We note, however, that the New Zealand Law Commission has recommended changes to New Zealand’s public register provisions. NZLC Report 101.

8.19 The Office of the Victorian Privacy Commissioner (OVPC) has reviewed the application of this provision in relation to building registers.<sup>33</sup> The report essentially proposed that, in order to administer building registers “so far as is reasonably practicable” in accordance with the IPPs, a clear statement of the purpose of the registers was necessary.<sup>34</sup> Further, the report found that there were “uses” that were not “purposes” of the register.<sup>35</sup> These uses were to be allowed on the condition that the individual concerned opt-in to direct marketing, and that the statistics were de-identified. It was especially relevant that these uses served an identifiable public interest and were not contrary to the objects of the legislation. Concerns were also raised about other possible uses such as identity fraud, stalking and harassment.<sup>36</sup> It was argued that the ability to suppress information contained on the register (similar to that under s 58 of PPIPA) and limiting the information that was to be placed on the register to only that which was necessary (such as names of building owners) would be sufficient to meet these concerns.<sup>37</sup>

8.20 The Victorian approach, then, is to regulate public registers through the “reasonably practicable” application of the general (non-public register specific) privacy principles and through register-specific provisions contained in the parent Act, by code or by regulation.<sup>38</sup> These register-specific provisions, whatever their vehicle, provide guidance on, and interpretation of, the privacy principles.

---

33. Office of the Victorian Privacy Commissioner, *Public Registers and Privacy: Building Permit Data* (2002).

34. Office of the Victorian Privacy Commissioner, *Public Registers and Privacy: Building Permit Data* (2002) Recommendation 1.

35. Namely, direct marketing and compilation of industry statistics. Office of the Victorian Privacy Commissioner, *Public Registers and Privacy: Building Permit Data* (2002) Recommendation 2.

36. Office of the Victorian Privacy Commissioner, *Public Registers and Privacy: Building Permit Data* (2002) [96].

37. Office of the Victorian Privacy Commissioner, *Public Registers and Privacy: Building Permit Data* (2002) [96]-[100], Recommendation 3.

38. Office of the Victorian Privacy Commissioner, *Public Registers and Privacy: Building Permit Data* (2002) [100]-[157].

## New Zealand

8.21 A similar “so far as is reasonably practicable” provision exists in the *Privacy Act 1993* (NZ) with regard both to privacy principles and Public Register Privacy Principles (“PRPPs”).<sup>39</sup> There are four PRPPs:<sup>40</sup>

- Principle 1 Search references: Personal information shall be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organised.
- Principle 2 Use of information from public registers: Personal information obtained from a public register shall not be re-sorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.
- Principle 3 Electronic transmission of personal information from register: Personal information in a public register shall not be made available by means of electronic transmission, unless the purpose of the transmission is to make the information available to a member of the public who wishes to search the register.
- Principle 4 Charging for access to public register: Personal information shall be made available from a public register for no charge or for no more than a reasonable charge.

8.22 The general consensus on the operation of these PRPPs is that they are unclear and are difficult to apply in practice.<sup>41</sup> The New Zealand Law Commission has thus recommended a move to regulation primarily through the statutes that establish the individual public registers.<sup>42</sup> Relevant IPPs would be incorporated by reference into the establishing Acts. The *Privacy Act 1993* (NZ) would thus cease to function as the regulating vehicle for public registers.

---

39. *Privacy Act 1993* (NZ) s 60(1). PRPPs relate only to public registers and operate in addition to the IPPs.

40. *Privacy Act 1993* (NZ) s 59.

41. See NZLC Report 101, [3.22]-[3.42], [3.74]-[3.75], [5.9]; G Murphy, “A local authority perspective” (1998) 5 *Privacy Law and Policy Reporter* 122, J Edwards, “Public registers: NZ’s approach” (1994) 1 *Privacy Law and Policy Reporter* 85.

42. NZLC Report 101, [5.15-5.23], Recommendation 1.

## Commonwealth

8.23 The *Privacy Act 1988* (Cth) does not seek to regulate public registers at the agency level; rather, it relies on the National Privacy Principles (“NPPs”) to regulate the conduct of those who access public registers. The ALRC has recommended that legislation establishing public registers clearly set out restrictions on electronic publication of personal information,<sup>43</sup> and has recommended that the Office of the Commonwealth Privacy Commissioner issue guidance relating to generally available publications in an electronic format.<sup>44</sup> The situation in NSW differs as PPIPA only applies to the public sector and thus can only regulate “end-users” insofar as they are public sector agencies.

## POSSIBLE METHODS OF PUBLIC REGISTER REGULATION

8.24 In any consideration of the ways in which public registers should be regulated, it is important to focus on the broad, high-level principles governing public registers and to keep in mind the purposes of public registers and thus the purposes of their regulation. There are, in our view, three options:

- (1) Repeal Part 6 in its entirety and regulate public registers solely through the UPPs (“UPP regime”).
- (2) Repeal Part 6 in its entirety and regulate public registers solely through their establishing statutes (“statute regime”).
- (3) Regulate public registers through the UPPs and where appropriate retain separate provisions in privacy legislation relating to public registers, namely s 58 (suppression), but reverse s 59 and allow regulation by their establishing statutes (“concurrent regime”).

### UPP regime

8.25 The adoption of the proposed UPPs, the removal of the exemption of “publicly available publications” and the exclusion of public registers from the definition of “generally available publication” will mean that public registers will be subject to the UPPs. This means that agencies

---

43. ALRC Report 108, vol 1, Recommendation 11-2.

44. ALRC Report 108, vol 1, Recommendation 11-1.

maintaining public registers would not be exempted from disclosure requirements under the proposed UPPs, as UPP 5.1(a)(i) still requires the secondary purpose to be “related to the primary purpose of collection”. While this is different from the test in s 57, where the disclosure must “relat[e] to the purpose of the register or the Act under which the register is kept”, it is arguable that in the majority of cases the two definitions would have the same effect. For example, the information collected for the Torrens register is collected for the purposes of the *Real Property Act 1900* (NSW).

8.26 The agency has the further burden of the requirements in UPP 5.1(a)(ii), that:

the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose and the agency has no reason to believe that the individual would object.

8.27 This would require the agency to notify the individual of the uses to which his or her personal information may be put and to gain his or her general consent to these uses. This is not an onerous requirement and we see no reason why the information that is to be contained on public registers should be treated any different in this respect to that used or disclosed for other agency purposes.

8.28 This option would have the benefit that public registers would be subject to the UPPs on data security and data quality. It would also mean that all personal information would be regulated under the same uniform privacy regime. These benefits are not to be underestimated.

8.29 However, public registers serve a particular public purpose. This particularity is not adequately dealt with by the UPPs. We have recognised this in other parts of this report, for example, in our discussion of “sector-specific” interpretation with regard to privacy codes.<sup>45</sup> It is unclear to what extent codes will be successful in regulating public registers since, under our proposals, codes would only be able to add to privacy protection, not decrease it. There may be a need for derogation from certain UPPs, for example, relating to the internet disclosure of certain personal information on a public register.<sup>46</sup>

---

45. See para 7.15.

46. For example, the names and qualifications of doctors or other health professionals.

8.30 Register-specific codes could, however, provide guidance on how different types of information (for example names, addresses, driving history, health information) should be specifically dealt with. It has been suggested in New Zealand that the content of each public register should be specified; for example, the rates roll should only include the property and the associated rate, not the name of the property owner or their postal address, since the rates apply to the property, not the owner. This does not necessarily mean that the name or postal address of the owner cannot be collected or stored by the agency, only that that information need not be included on the publicly available register.<sup>47</sup>

8.31 The limitations of code regulation could be overcome by the inclusion of a “reasonableness” provision similar to s 16(4) of the *Information Privacy Act 2000* (Vic).<sup>48</sup> Codes could be used to provide guidance as to the circumstances in which it is not “reasonably practicable” to comply with the privacy principles, for example with respect to internet access to public registers. We are of the view that a provision like s 16(4) may be interpreted too broadly and that any derogation from privacy principles should be enumerated more specifically.

8.32 The proposed specificity of interpretation could, of course, be achieved by the regulation-making power under s 71 of PPIPA.<sup>49</sup> This would require consultation with the users of each public register, the Privacy Commissioner, and the agency maintaining that register. This solution would be akin to the concurrent regime, except the specific regulation would be centralised in regulations made pursuant to PPIPA and not in the establishing statutes.

8.33 It is, in our view, more appropriate for register-specific provisions to be located in the establishing statute of that public register. This would authorise exemptions from the UPPs under the “required or authorised by law” exemption (for example UPP 5.1(e)) and would have the benefit of authorising derogation from privacy principles through specific legislation. This would have the further benefit of allowing the purposes of each public register to be clearly spelt out in its establishing statute.

---

47. G Murphy, “A local authority perspective” (1998) 5 *Privacy Law and Policy Reporter* 122, 123.

48. See para 8.18-8.20.

49. See para 7.4-7.14.

## Statute regime

8.34 Regulation of public registers entirely through their establishing statutes would provide the benefit of register-specific regulation. It would also result in certainty both as to the source of regulation and the obligations imposed by that regulation. It is for these reasons that the New Zealand Law Commission (“NZLC”) recommended a similar approach.<sup>50</sup>

8.35 Currently, however, there is little to no regulation of public registers by the statutes that establish them. This would mean that, as recognised by the NZLC,<sup>51</sup> a lot of work would have to be done on each public register, defining purposes, contemplated uses or users, and so on.

8.36 Additionally, and more importantly, the statute regime would recognise not only that public registers raise special problems for privacy, but would further assert that these problems are such that they should not be dealt with under the same legislative framework. In light of the recommendation for uniformity and consistency, it does not seem appropriate to regulate personal information wholly differently merely because it is contained within a public register. This would lead to a level of fragmentation which is both undesirable and unnecessary. The proposed UPPs are meant to act as a baseline minimum upon which further layers of privacy protection can be placed. As such, we believe that public registers should also be subject to the UPPs. This has been implicitly recognised by submissions that call for public registers to be governed by both the IPPs and Part 6.<sup>52</sup>

## Concurrent regime

8.37 The issues outlined above concerning both the UPP regime and the statute regime, namely, the issue of over-centralisation and the issue of lack of centralisation, can be addressed by a concurrent regime. This would mean that public registers would be subject to the UPPs, but that additional regulation would be achieved through a register’s establishing statute. This would both create an impetus for register-specific regulation, and allow in the interim for there to be some regulation of public

---

50. NZLC Report 101, [5.15]-[5.23], Recommendation 1.

51. NZLC Report 101, [5.18]-[5.19].

52. Australian Privacy Foundation, *Submission to the NSW Attorney General’s Department Review of the Privacy and Personal Information Protection Act 1998* (2004) 11.



registers. PIDs could be used in this interim period to ensure a smooth transition.

8.38 The NZLC expressed reservations about the way that a concurrent regime would operate, and the possibly confusing or uncertain “interplay” between the IPPs, PRPPs, other *Privacy Act 1993* (NZ) provisions and the provisions of an establishing statute.<sup>53</sup> While we acknowledge that having multiple sources of regulation has the potential for conflict and confusion, we do not believe that the achievement of uniform privacy legislation can occur with respect to regulation of public registers without the proposed UPPs applying to public registers. We also note that the New Zealand regime refers to the overlapping of four separate regulation sources, whereas under our proposal there will be only two. Further, part of the method or structure of the proposed uniform legislation is for “compliance-oriented regulation”,<sup>54</sup> that is, for privacy to be incorporated into agency thinking from the beginning, not just at the end.<sup>55</sup> This will mean that compliance with the UPPs becomes, in effect, automatic, or something that occurs as a matter of course.

8.39 We envisage a two-pronged approach to regulation through establishing statutes:

- First, by the regulation of end users, through methods such as the limitation of lawful uses of the information contained on the register.
- Secondly, by regulating the disclosure and security of the personal information by the public sector agency. This would be achieved by looking at what kinds of personal information are required to be held on the register, and what kinds of personal information need to be made public, in what form, and by what methods.

8.40 An example of the first approach is the *Corporations Act 2001* (Cth) which sets out limits on the use of personal information contained in registers established under that Act.<sup>56</sup> This would, of course, require the purposes of the register to be made clear in its establishing statute. As we

---

53. NZLC Report 101, [5.8].

54. ALRC Report 108, vol 1, [4.19]-[4.26].

55. ALRC Report 108, vol 1, ch 4.

56. Office of the Commonwealth Privacy Commissioner, *Consultation Paper for Information Sheet: Privacy and Collection of Publicly Available Personal Information* (2002) [22].

have outlined above, the purposes of several registers maintained by local councils have been set out in the Model Privacy Management Plan for Local Government. An example of the second approach is the *Medical Practice Act 1992* (NSW) which provides for the establishment of the Register of Medical Practitioners for NSW.<sup>57</sup> It further provides that only “such particulars of the registration of each registered medical practitioner as the [Medical] Board considers appropriate” are to be recorded.<sup>58</sup> These can be prescribed by regulation. This may entail, for example, that larger amounts of personal information could be accessed in person, and that access to public registers on the internet would be limited both in terms of the personal information made available and the method by which it is accessed.

8.41 The interplay between these two methods of regulation would ensure, first, that only the minimum amount necessary of personal information is made public, and secondly that this information is protected from misuse.

8.42 For regulation by establishing statutes to be effective, the provisions of those establishing statutes would have to prevail over the provisions of PPIPA. This would mean that s 59 would have to be repealed. The establishing statutes would then fall under the “required or authorised by law” exceptions from the UPPs. This would further reduce the potential for complexity and confusion arising from the “interplay” between various sources of regulation.

8.43 If this option is adopted, there would be no need to include in PPIPA a provision that public registers must comply with the privacy principles “where reasonably possible” similar to s 16(4) of the *Information Privacy Act 2000* (Vic). The generality and consequent potential for abuse of this exemption means that its purposes are better served by specific provisions contained in establishing statutes.

8.44 The essence of reform in this area, as we have emphasised previously, is that the purposes and intended uses of each public register be made clear, and that the regulation of each public register is crafted towards those purposes. In light of this, we believe that the best method of regulation, given the general goal of uniformity in privacy legislation, is for the proposed UPPs to apply as a baseline measure to public

---

57. *Medical Practice Act 1992* (NSW) sch 1 cl 21.

58. *Medical Practice Act 1992* (NSW) sch 1 cl 22(1).

registers, and for specific regulation to be implemented through a public register's establishing statute.

8.45 If the UPPs are not adopted, the general approach of co-regulation between PPIPA and the establishing statutes of registers should still be adopted. This would necessitate the amendment of s 59 to state that the provisions of establishing statutes prevail over the provisions of PPIPA in the case of inconsistency. It would also require statutory clarification that personal information contained in public registers is subject to the IPPs. In order to provide for greater flexibility in the disclosure of information from public registers, s 57 should be amended to include a "so far as reasonably practicable" test similar to s 16(4) of the *Information Privacy Act 2000* (Vic).

---

#### RECOMMENDATION 8.3

Public registers should be subject to the UPPs.

---

#### RECOMMENDATION 8.4

If Recommendation 8.3 is adopted, s 59 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

---

#### RECOMMENDATION 8.5

If the UPPs are not adopted, public registers should be subject to the IPPs. Section 57 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to say that "a public sector agency must, in administering a public register, so far as is reasonably practicable not perform an act or engage in a practice that would contravene an IPP in respect of information collected, held, managed, used, disclosed or transferred by it in connection with the administration of the public register".

---

**RECOMMENDATION 8.6**

If the UPPs are not adopted, s 59 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that the requirements of the law under which the public register concerned is established prevail to the extent of any inconsistency with the *Privacy and Personal Information Protection Act 1998* (NSW).

---

**RECOMMENDATION 8.7**

A review should be undertaken of the establishing statutes of all public registers in order to establish their purpose and proposed form of regulation.

9.

## **Enforcement mechanisms**

- Introduction
- Complaint resolution
- Data breach notification
- Role of criminal law

## INTRODUCTION

9.1 The proposed Unified Privacy Principles (“UPPs”) are stated at a high level of generality and implementation will depend on mechanisms and processes at a State level. The enforcement mechanisms adopted in NSW legislation and the role of the Privacy Commissioner are necessarily questions that must be addressed from a NSW perspective, despite the fact that these would occur within a potential national framework. Chapters 9-12 examine the enforcement of privacy legislation in NSW and propose changes to improve the efficacy of the current enforcement regime.

9.2 In this chapter we examine, broadly, the question of what enforcement mechanisms should be available under NSW privacy legislation. We consider in particular:

- the way in which complaints are resolved under privacy legislation and whether this should be modified in any way;
- the possibility of including data breach notification provisions in privacy legislation, as proposed by the Australian Law Reform Commission (“ALRC”); and
- the role of criminal law in the context of privacy legislation.

9.3 We preface our treatment of these issues with the obvious point that the mechanisms and processes that can be put in place depend on the resources available. The efficacy of the enforcement environment depends on the ability of the Privacy Commissioner to fulfil his or her functions. If the issue of chronic underfunding is addressed,<sup>1</sup> for example,

---

1. Privacy NSW’s resource issues have been noted on numerous occasions: “Privacy NSW does not have the resources required to carry out their tasking under the PIPP Act”: Privacy NSW, *Annual Report 2001-02* (2003) 69 (quoting from the “Andersen Report”, an independent resource review of Privacy NSW conducted during 2001-2002, funded by the Attorney General’s Department); “[W]e submit that the effectiveness of the Commissioner and Privacy NSW has been seriously limited by lack of resources ... the Commissioner’s office is hardly enlarged from its predecessor the Privacy Committee, which had a much more limited range of functions. Compared to privacy regulatory agencies in equivalent jurisdictions ... Privacy NSW is significantly under-resourced”: Australian Privacy Foundation, *Submission to the NSW Attorney General’s Department Review of the Privacy and Personal Information Protection Act 1998* (2004) 8; “[T]he NSW Office of the Privacy Commissioner is significantly under-resourced, impeding the effective resolution of privacy complaints by

through the adoption of our recommendations in Report 125,<sup>2</sup> there will be more flexibility in the range of enforcement mechanisms that can be engaged.

## COMPLAINT RESOLUTION

### Current approach

9.4 Currently, “a person who is aggrieved by the conduct of a public sector agency” can require an agency to carry out an internal review in certain circumstances.<sup>3</sup> Enforcement of the Information Protection Principles (“IPPs”) in the *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”) is therefore primarily through internal review of the conduct or decision. A person dissatisfied with the findings of an internal review may apply to the Administrative Decisions Tribunal (“ADT”) for external review of the conduct that was the subject of an internal review by the agency.<sup>4</sup> This can result in binding findings and enforceable remedies.<sup>5</sup> A party to the proceedings may appeal to an Appeal Panel against a decision or order of the Tribunal.<sup>6</sup>

9.5 PPIPA also allows for complaints to be made to the Privacy Commissioner where there has been “an alleged violation of, or interference with, the privacy of an individual”.<sup>7</sup> The subject matter of a

---

consumers, such complaints are typified by significant delays in case management and waiting lists”: Combined Community Legal Centres’ Group (NSW) Inc, *Submission on the Draft Report, Investigation into the Burden of Regulation in NSW and Improving Regulatory Efficiency* (IPART, 2008) 3, <[www.ipart.nsw.gov.au](http://www.ipart.nsw.gov.au)> at 16 December 2009. See also C Puplick, “NSW Privacy Commissioner Rejects Ministerial Interference” (2002) 9(7) *Privacy Law and Policy Reporter* 133, 135.

2. NSW Law Reform Commission, *The Offices of the Information and Privacy Commissioners*, Report 125 (2009).
3. *Privacy and Personal Information Protection Act 1998* (NSW) s 53. The circumstances are outlined in s 52. This includes contravention of an IPP, privacy code of practice, as well as disclosure of personal information kept in a public register.
4. *Privacy and Personal Information Protection Act 1998* (NSW) s 55.
5. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(2); *Administrative Decisions Tribunal Act 1997* (NSW) s 63-66.
6. *Privacy and Personal Information Protection Act 1998* (NSW) s 56.
7. *Privacy and Personal Information Protection Act 1998* (NSW) s 45. See also s 36(2)(k).

complaint may relate to conduct to which internal and external review applies. However, the scope of this avenue of redress is broader than the breach of IPPs by a public sector agency. The Privacy Commissioner's powers following a complaint are limited to inquiry and investigation, conciliation and reporting.<sup>8</sup>

9.6 While there are two avenues for complaint resolution under PPIPA, there is no requirement that complainants make a choice.<sup>9</sup> However, "as a matter of practice", the time limits imposed by the legislation are "usually such that the complainant has little ability to gain the benefit of an investigation by the Privacy Commissioner before seeking internal review".<sup>10</sup> External review by the ADT can only be conducted after a request for internal review.<sup>11</sup>

9.7 Under the *Health Records and Information Privacy Act 2002* (NSW) ("HRIPA") a different enforcement framework applies to the private sector. This is discussed below.<sup>12</sup>

---

8. See para 11.28-11.49.

9. In the second reading speech, the then Attorney General stated: "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": New South Wales, *Parliamentary Debates*, Legislative Council, 17 September 1998, 7599-7602 (Hon JW Shaw, Attorney General).

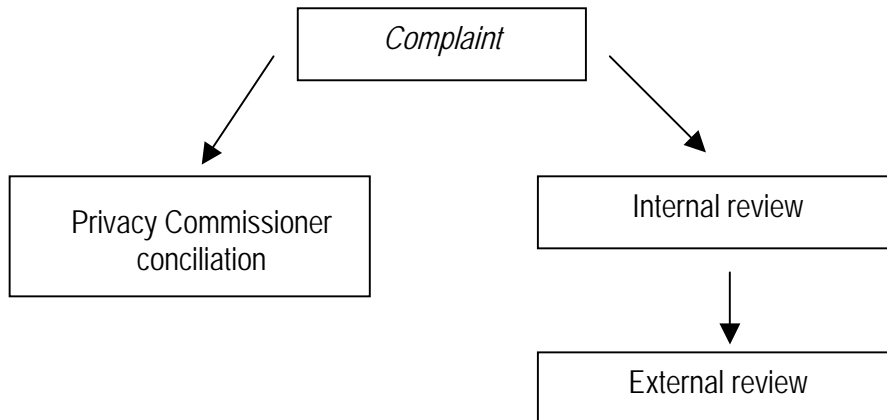
10. In practice, complainants are asked to make a choice between either internal review or conciliation: Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 107.

11. See *PC v University of New South Wales* [2005] NSWADTAP 72, [21].

12. See para 9.12. Note that we recommend that the *Health Records and Information Privacy Act 2002* (NSW) should be repealed: Recommendation 1.1.



Figure 1: Current complaint resolution process



### How should complaints be resolved?

9.8 In CP 3 we considered the appropriateness of the current method of resolving complaints, including whether the ADT is an appropriate forum for privacy disputes.<sup>13</sup> The ADT has expressed a preference for final determination by the Privacy Commissioner.<sup>14</sup> We note in CP 3 that final determination by the Privacy Commissioner may be advantageous because:<sup>15</sup>

- the specialisation offered by the Commissioner will be useful when determining privacy disputes;
- the Commissioner will have access to more flexible resources;
- the Commissioner will have experienced investigative staff that have credibility with agencies, whereas the ADT has no investigative staff;
- the ADT process can be complicated and expensive;
- self-represented litigants can prolong proceedings in the ADT;
- and

13. See NSW Law Reform Commission, *Privacy Legislation in New South Wales*, Consultation Paper 3 (2008) (“NSWLRC CP 3”) [7.46]-[7.50].

14. NSW Administrative Decisions Tribunal, *Submission to the Attorney General’s Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (2004) 7. See also NSWLRC CP 3, [7.46].

15. See NSWLRC CP 3, [7.46]-[7.49]. See also NSW Administrative Decisions Tribunal, *Submission to the Attorney General’s Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (2004).

- cases in the ADT are minor ones based on technical points, whereas the serious cases are often mediated.

9.9 We also asked whether Part 5 of PPIPA should be amended to give final determination of a complaint to the Privacy Commissioner rather than the ADT.<sup>16</sup> Many of the submissions that responded to this issue were forcefully opposed to a model where the Privacy Commissioner is capable of making final determinations.<sup>17</sup> These submissions noted that:

- Privacy NSW has been under resourced for many years;<sup>18</sup>
- the Commissioner final determination model is too reliant on government funding;<sup>19</sup>
- cases often arise on complex points of statutory interpretation and these are more appropriately addressed by the ADT;<sup>20</sup>
- the Privacy Commissioner “[a]lready has competing roles with respect to education, advice and research” and placing the Commissioner in a quasi-judicial role “would create too great a conflict with respect to those other roles, and the more proactive work would likely suffer as a result”;<sup>21</sup>
- it is “a fundamental matter of justice that the Privacy Commissioner’s determinations be open to review”;<sup>22</sup>
- ADT determination allows for the development of a body of case law that the Privacy Commissioner can use as guidance;<sup>23</sup>

---

16. NSWLRC CP 3, Issue 61.

17. Australian Privacy Foundation, *Submission*, 14; Business Law Committee of the Law Society, *Submission*, 15; Cyberspace Law and Policy Centre, *Submission*, 34; HIV/AIDS Legal Centre, *Submission*, 13; Inner City Legal Centre, *Submission*, 43; Public Interest Advocacy Centre, *Submission*, 32. The NSW FOI/Privacy Practitioners’ Network, *Submission*, 12 notes that the Network is unsure about the best model however it cautions that changing the model may not result in improvement. Privacy NSW, *Submission*, 13, reserved comment until the Commonwealth model emerges.

18. Cyberspace Law and Policy Centre, *Submission*, 34; HIV/AIDS Legal Centre, *Submission*, 13; Public Interest Advocacy Centre, *Submission*, 32.

19. Public Interest Advocacy Centre, *Submission*, 32.

20. Public Interest Advocacy Centre, *Submission*, 32.

21. Cyberspace Law and Policy Centre, *Submission*, 34.

22. Inner City Legal Centre, *Submission*, 43.

23. Inner City Legal Centre, *Submission*, 43. See also Public Interest Advocacy Centre, *Submission*, 32.

- the Commonwealth Privacy Commissioner has rarely exercised the power to make a determination leading to “almost complete absence of a comparable body of jurisprudence under the *Privacy Act 1988* (Cth)”;<sup>24</sup> and
- individuals require “reasonable recourse to a body with arbitral powers, capable of making binding findings” and such findings should be subject to appeal.<sup>25</sup>

9.10 Conversely, Legal Aid NSW expressed concern with the tribunal-based resolution of complaints where “most applicants are unrepresented and are pursuing remedies that do not involve significant damages”.<sup>26</sup> It noted that privacy litigation in the ADT is often delayed by technical challenges and “inexpert preparation and presentation of cases by unrepresented applicants”.<sup>27</sup> Legal Aid further noted that “greater emphasis on litigation can be seen to run counter to the trend in other areas of law to promote alternative dispute resolution processes”.<sup>28</sup>

9.11 Several submissions suggested adopting a “hybrid model” with the option of either internal review or determination by the Privacy Commissioner with the right of appeal to the ADT from both avenues.<sup>29</sup>

## Alternative models

### *HRIPA*

9.12 While complaints against public sector agencies under HRIPA are handled under the internal and external review provisions of PPIPA,<sup>30</sup> complaints against private sector persons are handled in a different manner. Complaints against private sector persons can be made to the

---

24. Public Interest Advocacy Centre, *Submission*, 32.

25. HIV/AIDS Legal Centre, *Submission*, 13.

26. Legal Aid NSW, *Submission*, 5.

27. Legal Aid NSW, *Submission*, 6.

28. Legal Aid NSW, *Submission*, 5.

29. Australian Privacy Foundation, *Submission*, 14; Cyberspace Law and Policy Centre, *Submission*, 34.

30. Under *Health Records and Information Privacy Act 2002* (NSW) s 21 complaints against public sector agencies relating to contraventions of an HPP or health privacy code of practice is conduct to which *Privacy and Personal Information Protection Act 1998* (NSW) pt 5 applies (provisions relating to internal review). References in pt 5 to: personal information includes health information; IPP includes HPP; and privacy code includes a health privacy code of practice.

Privacy Commissioner in relation to a contravention of a Health Privacy Principle (“HPP”); a provision of Part 4 of HRIPA; or a health privacy code of practice.<sup>31</sup> After conducting a preliminary assessment of the complaint, the Privacy Commissioner may decide not to deal with it if satisfied of one of a number of factors.<sup>32</sup> If the Privacy Commissioner is satisfied that there is a *prima facie* case of a breach of HRIPA,<sup>33</sup> the Commissioner may endeavour to resolve the complaint by conciliation; further investigate the complaint and make a report; or determine that the complaint has been resolved to his or her satisfaction.<sup>34</sup> 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 (a written report of findings or recommendations).<sup>35</sup> The complaint is heard in the ADT’s original jurisdiction and the ADT can make legally binding orders, including costs orders.<sup>36</sup>

### *Commonwealth*

9.13 Under the *Privacy Act 1988* (Cth), the Commonwealth Privacy Commissioner is required to “investigate an act or practice of an agency that may breach an Information Privacy Principle and, where the Commissioner considers it appropriate to do so, to endeavour, by conciliation, to effect a settlement of the matters that gave rise to the investigation”.<sup>37</sup> Where conciliation is successful, the Commonwealth Privacy Commissioner can close the file if he or she feels that the respondent has adequately dealt with the matter.<sup>38</sup> The Commonwealth Privacy Commissioner may also close the file where conciliation is unsuccessful but the respondent has made a reasonable offer.<sup>39</sup> If the Commonwealth Privacy Commissioner feels that a reasonable offer has

---

31. *Health Records and Information Privacy Act 2002* (NSW) s 42.

32. *Health Records and Information Privacy Act 2002* (NSW) s 43.

33. *Health Records and Information Privacy Act 2002* (NSW) s 44.

34. *Health Records and Information Privacy Act 2002* (NSW) s 42.

35. *Health Records and Information Privacy Act 2002* (NSW) s 48.

36. *Health Records and Information Privacy Act 2002* (NSW) s 54, s 55.

37. *Privacy Act 1988* (Cth) s 27(1)(a).

38. See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”) vol 2, [49.41].

39. ALRC Report 108, vol 2, [49.42].

not been made and finds the complaint substantiated, he or she can make a determination declaring:<sup>40</sup>

- the respondent has engaged in conduct that constitutes an interference with the privacy of an individual and should not repeat or continue such conduct;<sup>41</sup>
- the respondent should perform a reasonable act or engage in a course of conduct to redress any loss or damage suffered by the complainant;<sup>42</sup>
- the complainant is entitled to compensation for loss or damage suffered due to act or practice;<sup>43</sup> or
- it would be inappropriate for any further action to be taken in the matter.<sup>44</sup>

9.14 A determination is not binding on either party. The determination may, however, be enforced through the Federal Court or the Federal Magistrates Court.<sup>45</sup>

9.15 The ALRC has recommended that where there have been reasonable attempts to conciliate a complaint and the Commonwealth Privacy Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify both parties that conciliation has failed. Either party may then require that the complaint be resolved by determination.<sup>46</sup> Currently, the Administrative Appeals Tribunal (“AAT”) has the power to review a

---

40. See ALRC Report 108, vol 2, [49.42]-[49.43].

41. *Privacy Act 1988* (Cth) s 52(1)(b)(i).

42. *Privacy Act 1988* (Cth) s 52(1)(b)(ii).

43. *Privacy Act 1988* (Cth) s 52(1)(b)(iii).

44. *Privacy Act 1988* (Cth) s 52(1)(b)(iv).

45. *Privacy Act 1988* (Cth) s 55A.

46. See ALRC Report 108, vol 2, Recommendation 49-5. The ALRC further recommends that the Act be amended to empower the Commonwealth Privacy Commissioner to compel parties to a complaint and any other relevant person to attend a compulsory conference (previously limited to agencies): ALRC Report 108, vol 2, Recommendation 49-11, [49.121]. The ALRC also recommends that the Commonwealth Privacy Commissioner be empowered to direct that hearing for a determination be conducted without oral submissions from parties if he or she is satisfied that the matter could be determined fairly on the basis of written submissions by the parties: ALRC Report 108, vol 2, Recommendation 49-13.

small subset of declarations.<sup>47</sup> The ALRC has recommended that the *Privacy Act 1988* (Cth) be amended to allow merits review of all determinations made by the Commonwealth Privacy Commissioner.<sup>48</sup> The ALRC believes that this “may provide an alternative, and less costly, ‘enforcement’ mechanism for complainants than is currently provided under the Act”.<sup>49</sup>

### *The GIPA Act*

9.16 Under the *Government Information (Public Access) Act 2009* (NSW) (the “GIPA Act”), the Information Commissioner is empowered to review particular decisions by agencies<sup>50</sup> and make “recommendations” upon review.<sup>51</sup> The ADT can review recommendations of the Information Commissioner, and internal review decisions of an agency.<sup>52</sup> The powers of the Information Commissioner to prevent contraventions of an “Information Act”<sup>53</sup> is outlined in s 28 of the *Government Information (Information Commissioner) Act 2009* (NSW).

9.17 The Information Commissioner also has the power to conciliate complaints about the exercise of agency functions under an Information Act, “including conduct that is alleged by the person to constitute contravention of an Information Act”.<sup>54</sup> However, a decision of an agency that is reviewable under the GIPA Act cannot be the subject of a complaint to the Information Commissioner.<sup>55</sup>

---

47. An application can be made to the AAT for review of declarations for compensation or refusals to make such declarations (“merits review”). This is only applicable to agencies: *Privacy Act 1988* (Cth) s 61. See ALRC Report 108, vol 2, [49.75].

48. See ALRC Report 108, vol 2, Recommendation 49-7.

49. ALRC Report 108, vol 2, [50.23].

50. *Government Information (Public Access) Act 2009* (NSW) s 80, pt 4 div 3.

51. *Government Information (Public Access) Act 2009* (NSW) s 89.

52. *Government Information (Public Access) Act 2009* (NSW) s 100. Note that a reviewable decision does not have to be internally reviewed or reviewed by the Information Commissioner before it can be the subject of an ADT review.

53. An Information Act is the *Government Information (Public Access) Act 2009* (NSW) and any other Act that is declared by the regulations to be an Information Act for the purposes of the *Government Information (Information Commissioner) Act 2009* (NSW): *Government Information (Information Commissioner) Act 2009* (NSW) s 3.

54. *Government Information (Information Commissioner) Act 2009* (NSW) s 17.

55. *Government Information (Public Access) Act 2009* (NSW) s 89(4).

*Ombudsman Act 1974 (NSW)*

9.18 Under the *Ombudsman Act 1974* (NSW) the Ombudsman may make a “report of an investigation” where he or she finds that the conduct that was the subject of the investigation satisfies particular criteria.<sup>56</sup> The Ombudsman can recommend a number of things, including that the conduct be reconsidered; actions be taken to rectify the conduct or consequences; or compensation be made.<sup>57</sup> The report must be given to the responsible Minister; the head of the authority whose conduct is the subject of the report; and in some cases, the Department of Premier and Cabinet.<sup>58</sup>

9.20 The Ombudsman may attempt to deal with particular complaints by conciliation.<sup>59</sup> Participation is voluntary and, if the conciliation is unsuccessful, the “conciliator is excluded from participating as an investigating officer in any investigation of the complaint”.<sup>60</sup>

**The Commission’s view**

9.21 We agree with submissions that it is appropriate for final determination to remain with the ADT. However, we also wish to ensure that privacy legislation provides an accessible framework to deal expeditiously with privacy related complaints. Privacy NSW has recommended that “the ability to seek review by the [ADT] be expanded to include matters which could be the subject of internal review but for which the complainant instead sought an investigation by the Privacy Commissioner”.<sup>61</sup> This leaves open the possibility of expanding the powers of the Privacy Commissioner to include the power to make determinations with respect to particular complaints (which can be reviewed by the ADT).<sup>62</sup> Strengthening the role of the Privacy

---

56. *Ombudsman Act 1974* (NSW) s 26(1). For example, conduct that was contrary to law or unreasonable, unjust, oppressive or improperly discriminatory.

57. *Ombudsman Act 1974* (NSW) s 26(2).

58. *Ombudsman Act 1974* (NSW) s 26(3). Where the investigation arises out of a complaint, the Ombudsman may give a copy to the complainant and the authority to which the conduct relates: s 26(4).

59. *Ombudsman Act 1974* (NSW) s 13A.

60. *Ombudsman Act 1974* (NSW) s 13A(3), s 13A(5).

61. Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 124.

62. As noted by Privacy NSW, “one possibility is that the Privacy Commissioner could assist to narrow issues and make a prima facie determination before any

Commissioner would take advantage of the specialisation and accessibility of the Office. It could also provide for external review of a matter, without the matter necessarily being brought before the ADT. This may be of particular benefit to complainants as it has been argued that the ADT process advantages agencies.<sup>63</sup>

### *Commissioner determination*

9.22 It has been noted that “there is a clear distinction between those authorities whose powers are limited to those of investigation and recommendation, and those that can mandate changes in behaviour”.<sup>64</sup> The advisory role has the advantage of avoiding the “adversarial relationships that arise when enforcement powers are used or threatened”<sup>65</sup> and is likely to foster positive relationships between the Commissioner and agencies.<sup>66</sup> Conversely, the power to make orders or determinations “provides strong incentive to the parties to settle on reasonable terms”<sup>67</sup> and “the ability to negotiate with data users is facilitated by the existence of enforcement powers, even if those powers are rarely used”.<sup>68</sup> Further, a pure advisory or conciliatory role is less likely to result in a consistent approach to complaints handling and “the strengths of the ombudsman model, relying on influence, moral suasion and informality to ensure compliance and effect behavioural change,

---

matter reaches the Tribunal”: Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 124.

63. It has been noted that applicants are often unrepresented, whereas agencies are often “well represented, and better able to make arguments about statutory interpretation”: Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 119.
64. C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd ed, 2006) 143.
65. C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd ed, 2006) 143.
66. Canadian Government, *Access to Information: Making it Work for Canadians*, Report of the Access to Information Task Force (2002) 111.
67. G V La Forest, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*, Report of the Special Advisor to the Minister of Justice (Canada, Department of Justice, 2005) 50. See also A Bendall, “The Governance of Privacy: Speak softly and carry a big stick” (Paper presented to the 2008 Australian Institute of Administrative Law Forum, Melbourne, 8 August 2008) 12.
68. C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd ed, 2006) 143.



have been less evident in the last few years".<sup>69</sup> A determination power could also encourage faster resolution of complaints. It has been acknowledged that providing Privacy Commissioners with determination powers has worked well in some Canadian provinces.<sup>70</sup> It is possible that a determination power could encourage greater consistency, transparency and accountability.<sup>71</sup>

9.23 We certainly see merit in an approach that gives the Privacy Commissioner a determination power (reviewable by the ADT). However, as noted in the introduction, resources are a key issue that will impact upon the Commissioner's ability to perform his or her role. The appropriate approach will depend on many variables, including whether our recommendations with respect to the Office of the Information Commissioner<sup>72</sup> and statutory cause of action for invasion of privacy<sup>73</sup> are adopted. We must approach this issue in the current context, where the uncertainties surrounding the future of privacy law in NSW prevent us recommending with any confidence that the Privacy Commissioner be given the power to issue determinations. However, we believe that this matter should be kept under consideration, especially if there are significant changes to available resources.

9.24 In any reconsideration of the power of the Privacy Commissioner to issue determinations, the following questions should be considered:

- (1) In what circumstances can the Privacy Commissioner issue a determination?
- (2) Will the power to issue determinations conflict with the power to conciliate complaints?

---

69. Addressing Canada's FOI enforcement framework: Canadian Government, *Access to Information: Making it Work for Canadians*, Report of the Access to Information Task Force (2002) 112.

70. The powers are used sparingly, with a preference for conciliation, mediation and other informal means, where possible. See G V La Forest, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*, Report of the Special Advisor to the Minister of Justice (Canada, Department of Justice, 2005) 50.

71. C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd ed, 2006) 143.

72. See NSW Law Reform Commission, *The Offices of the Information and Privacy Commissioners*, Report 125 (2009).

73. NSW Law Reform Commissioner, *Invasion of Privacy*, Report 120 (2009).

- (3) Should the complainant or respondent be able to compel the Privacy Commissioner to issue a determination, as proposed by the ALRC?
- (4) Should a complainant or respondent only be able to appeal to the ADT where the Privacy Commissioner has issued a determination?
- (5) Should the ADT review a determination in their review jurisdiction or original jurisdiction?

*ADT trigger*

9.25 In the current context we recommend allowing external review by the ADT after the Privacy Commissioner notifies the complainant that the conciliation has failed.<sup>74</sup> This could only occur in reference to conduct that is reviewable under Part 5 of PPIPA.<sup>75</sup> This approach will provide a feasible alternative to complainants who may not be comfortable utilising internal review processes.<sup>76</sup> It will also ensure that complainants who unsuccessfully attempt to conciliate a complaint still have recourse to enforceable remedies.<sup>77</sup>

9.26 It is likely that the ADT would have to review the conduct under its “original” jurisdiction as no reviewable decision or determination has been made and the Tribunal is clearly the “primary decision maker”.<sup>78</sup> However, we also believe that external review by the ADT following a complaint to the Privacy Commissioner should be handled in a way consistent with the review processes following internal review by an agency.<sup>79</sup>

---

74. See Recommendation 11.8.

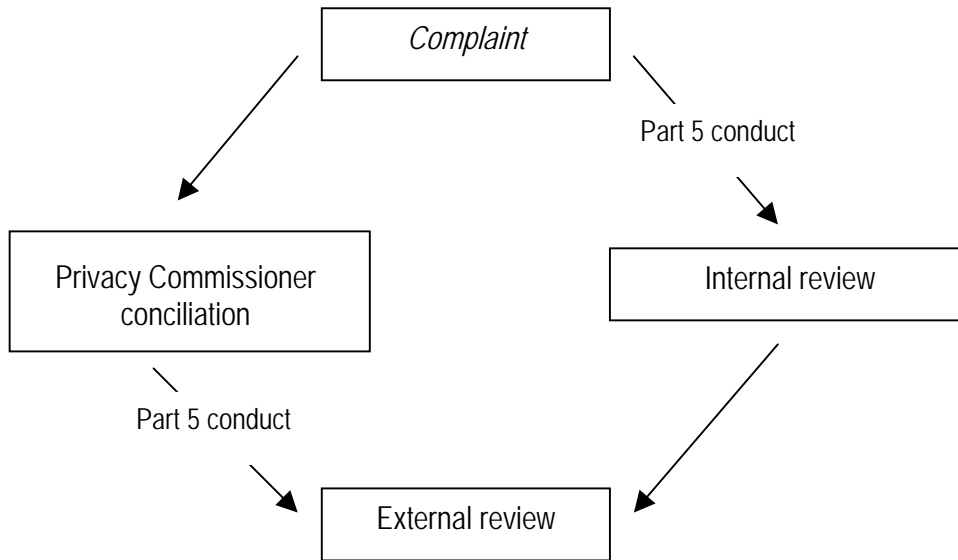
75. See Recommendations 9.2(4) and 12.1.

76. See Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 117.

77. See Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 108.

78. See para 12.19-12.22.

79. See Recommendations 12.9, 12.12. See also Recommendation 12.5(1).

*Figure 2: Proposed complaint resolution process***RECOMMENDATION 9.1**

Where a public sector agency has allegedly contravened an applicable IPP, privacy code of practice, public register provision, or proposed data breach notification provision, and the Privacy Commissioner notifies the complainant that conciliation has failed, the complainant should be able to apply to the Administrative Decisions Tribunal for external review of the agency's conduct.

**DATA BREACH NOTIFICATION****ALRC proposal**

9.27 The ALRC recommended the addition of a data breach notification provision in the *Privacy Act 1988* (Cth). Data breach notification is “in essence a legal requirement on agencies and organisations to notify individuals when a breach of security leads to the disclosure of personal information”.<sup>80</sup> The ALRC recommended that:<sup>81</sup>

The Privacy Act should be amended to include a new Part on data breach notification, to provide as follows:

80. ALRC Report 108, vol 2, [51.1].

81. ALRC Report 108, vol 2, Recommendation 51-1.

- (a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.
- (b) The definition of ‘specified personal information’ should include both personal information and sensitive personal information, such as information that combines a person’s name and address with a unique identifier, such as a Medicare or account number.
- (c) In determining whether the acquisition may give rise to a real risk of serious harm to any affected individual, the following factors should be taken into account:
  - (i) whether the personal information was encrypted adequately; and
  - (ii) whether the personal information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the Privacy Act (provided that the personal information is not used or subject to further unauthorised disclosure).
- (d) An agency or organisation is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.
- (e) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.

9.28 In arriving at this recommendation, the ALRC examined data breach notification laws adopted in various jurisdictions and the rationale for their implementation.<sup>82</sup> The rationales include:

- ***Reducing identity theft:*** notification helps to ensure that individuals mitigate risk and protect against consequences of identity theft.<sup>83</sup>

---

82. ALRC Report 108, vol 2, [51.3].

83. ALRC Report 108, vol 2, [51.4]-[51.7], [51.47].

- **Counteracting lack of market incentives to notify:** the market does not provide enough incentive to notify individuals regarding data breaches due to the costs of notification and the possibility of negative publicity.<sup>84</sup>
- **Creating incentives to secure data:** organisations may be more inclined to increase security because of the damage to reputation that can flow from data breach notification requirements.<sup>85</sup>
- **Addressing increased number of data breaches:** there has been an increasing number of data breaches, especially high profile breaches.<sup>86</sup>
- **Potential scope of harm from breach:** the harm from a data breach may not only be financial harm. Disclosure of certain types of personal information such as health information could lead to discriminatory treatment or damage to reputation.<sup>87</sup>
- **Counteracting information inadequacy:** breach notification is important because it will assist in keeping the market informed of the privacy practices of various organisations. This allows individuals to assess and compare information-handling practices.<sup>88</sup>
- **Accountability:** breach notification may “improve accountability, openness and transparency” in information handling.<sup>89</sup>

9.29 The ALRC recommended implementing data breach notification requirements applicable to both agencies and organisations noting that such a requirement can protect personal information from “any further exposure or misuse” and encourage transparency of information-handling practices.<sup>90</sup>

9.30 In developing a data breach regime, the following issues need to be addressed:

- the trigger for notification;

---

84. ALRC Report 108, vol 2, [51.8]-[51.9].

85. ALRC Report 108, vol 2, [51.10], [51.47].

86. ALRC Report 108, vol 2, [51.11]-[51.13].

87. ALRC Report 108, vol 2, [51.78].

88. ALRC Report 108, vol 2, [51.81].

89. ALRC Report 108, vol 2, [51.47].

90. ALRC Report 108, vol 2, [51.73].

- who should be responsible for notification;
- the definition of personal information;
- exceptions;
- content of notification;
- timing and method of notification; and
- penalties for a failure to notify.

*Trigger and responsibility for notification*

9.31 The proposed Commonwealth data breach notification provisions would operate separately from the requirements under the proposed UPPs. The requirements can thus be triggered in cases where an organisation has or has not complied with the privacy principles.<sup>91</sup> This is because the primary reason for the notification requirement is minimisation of damage caused by the breach.<sup>92</sup>

9.32 The ALRC recommends that the data breach provision should contain a requirement to notify the Privacy Commissioner and “affected individuals” where “specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person; and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual”.<sup>93</sup>

9.33 This test (“a real risk of serious harm”) sets a higher notification threshold than other jurisdictions. The ALRC believes that this will assist in minimising “notification fatigue”, which can occur where individuals receive frequent notifications and it becomes difficult to determine which ones carry a serious risk of harm.<sup>94</sup> The organisation or agency will decide whether notification requirements have been triggered but the ALRC suggests that this decision be made in consultation with the Commonwealth Privacy Commissioner and provides the Commissioner with an oversight power.<sup>95</sup> The ALRC believes that the oversight powers

---

91. ALRC Report 108, vol 2, [51.74]-[51.75].

92. ALRC Report 108, vol 2, [51.76].

93. ALRC Report 108, vol 2, [51.83].

94. ALRC Report 108, vol 2, [51.86].

95. ALRC Report 108, vol 2, [51.88].

given to the Commonwealth Commissioner will assist in identifying and addressing systemic issues.<sup>96</sup>

9.34 The ALRC believes that the data breach notification requirements should apply to breaches that occur within Australia (to all affected individuals) and also breaches outside Australia that are subject to the extraterritoriality provisions.<sup>97</sup>

#### *Personal information*

9.35 The ALRC suggests that data breach provisions apply to “specified personal information” and the definition of such information should “draw on the existing definitions of ‘personal information’ and ‘sensitive information’ in the *Privacy Act* and should prescribe what combinations of these types of information would, when acquired without authorisation, give rise to a real risk of serious harm requiring notification”.<sup>98</sup>

#### *Exceptions*

9.36 The ALRC discussed and rejected a model that lists specific exceptions to data breach notification, for example, where the information is encrypted. The ALRC notes that these “factors should be included as part of the assessment of whether there is a real risk of serious harm arising from the breach”.<sup>99</sup> It subsequently recommended that when determining whether there is serious harm, consideration should be given to whether the information acquired was encrypted and also whether the information was acquired in good faith.<sup>100</sup>

#### *Content and method of notification*

9.37 As a minimum, the ALRC suggests that the breach notification should contain a description of the breach, a list of the type of personal information disclosed and contact information for affected individuals to obtain further information and assistance.<sup>101</sup> The ALRC also suggest that

---

96. ALRC Report 108, vol 2, [51.89].

97. ALRC Report 108, vol 2, [51.106].

98. ALRC Report 108, vol 2, [51.96].

99. ALRC Report 108, vol 2, [51.91].

100. ALRC Report 108, vol 2, [51.91]-[51.94].

101. ALRC Report 108, vol 2, [51.100].

the Office of the Commonwealth Privacy Commissioner develop identity theft guidelines to assist in mitigating the risk of identity theft.<sup>102</sup>

9.38 The ALRC believes that the method of notification should be determined by the agency or organisation's "ordinary method of communicating with individuals".<sup>103</sup> The Commonwealth Privacy Commissioner should be empowered to approve substituted notice "where he or she believes it is appropriate, reasonable and fair in all the circumstances".<sup>104</sup>

### *Penalties*

9.39 The ALRC recommends imposing civil penalties for a failure to notify the Commonwealth Privacy Commissioner of a data breach.<sup>105</sup>

### **Difficulties when formulating data breach notification provisions**

9.40 The connection between data breaches and identity theft has been criticised as being overstated.<sup>106</sup> Commentators have indicated that "adoption of data breach disclosure laws have marginal effect on the incidences of identity thefts and reduce the rate by just under 2%, on average".<sup>107</sup> The issue is that while information security is of critical importance, security breaches may or may not be depending on the circumstances.<sup>108</sup> Breach provisions may lead to the modification of security practices of agencies or organisations concerned about the costs and poor publicity associated with a data breach.<sup>109</sup> However, the breach notification system is still essentially responsive rather than preventive.<sup>110</sup>

---

102. ALRC Report 108, vol 2, [51.101].

103. ALRC Report 108, vol 2, [51.102].

104. ALRC Report 108, vol 2, [51.103].

105. ALRC Report 108, vol 2, [51.108].

106. F Cate, M Abrams, P Bruening and O Swindle, *Dos and Don'ts of Data Breach and Information Security Policy* (Centre for Information Policy Leadership, 2009) 2.

107. S Romanosky, R Telang, A Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?* (Social Science Research Network, 2008) 1, <<http://ssrn.com/abstract=1268926>> (accessed 31 December 2009).

108. F Cate, *Information Security Breaches: Looking Back and Thinking Ahead* (Centre for Information Policy Leadership, 2008) 1.

109. See s Romanosky, R Telang, A Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?* (Social Science Research Network, 2008) 1, <<http://ssrn.com/abstract=1268926>> (accessed 31 December 2009).

110. F Cate, *Information Security Breaches: Looking Back and Thinking Ahead* (Centre for Information Policy Leadership, 2008) 6.



Any implementation of a data breach notification system should take this into account to ensure that the formulation efficiently allocates agencies' resources.

9.41 The ALRC model has been subject to criticism on the ground that an individual complainant cannot enforce data breach notification provisions. The model relies on the Commonwealth Privacy Commissioner to enforce the provisions "through an 'own motion' investigation and notice, with a civil penalty sanction for non-compliance".<sup>111</sup> It has also been criticised for being too subjective and therefore allowing for avoidance of disclosure of breaches based on the judgment of the party in breach.<sup>112</sup> It has further been suggested that data breach notification is most appropriately located within the proposed UPPs.<sup>113</sup>

### The Commission's view

9.42 We support the ALRC recommendation in principle. However, we depart from the ALRC in relation to the precise implementation of these provisions. Our suggested variations are discussed below.

#### *Personal Information*

9.43 The requirement that data breach notification provisions apply to "specified personal information" appears to add an unnecessary layer of complexity to data breach provisions. The provisions are already triggered where "the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual". The requirement that the information be "combinations of ... types of information [that] would, when acquired without authorisation, give rise to a real risk of serious harm"<sup>114</sup> appears redundant in this context.<sup>115</sup>

---

111. Cyberspace Law and Policy Centre, "Best practice privacy principles: suggested improvements to the ALRC's model unified privacy principles (UPPs)", *Submission to the Australian Government* (2008) 40. For further discussion regarding own motion investigations see para 10.17-10.24.

112. Cyberspace Law and Policy Centre, "Best practice privacy principles: suggested improvements to the ALRC's model unified privacy principles (UPPs)", *Submission to the Australian Government* (2008) 40.

113. Cyberspace Law and Policy Centre, "Best practice privacy principles: suggested improvements to the ALRC's model unified privacy principles (UPPs)", *Submission to the Australian Government* (2008) 40.

114. ALRC Report 108, vol 2, [51.96].

*Compliance*

9.44 We do not believe that civil penalties would be an appropriate sanction in the context of NSW government agencies. We think it would be more effective to ensure compliance in the same manner as contraventions of the IPPs. In most cases, we envisage that the Privacy Commissioner will use his or her proposed audit or own motion investigation power to enforce data breach notification provisions.<sup>116</sup> However, we also believe that individuals should be able to make complaints to the Commissioner where they believe a breach of notification provisions has occurred, or request that an agency conduct an internal review to determine if the agency acted appropriately.<sup>117</sup> If required, this can then be appealed to the ADT in the same manner as contravention of the IPPs or proposed UPPs. This could lead to, for example, the payment of compensation where appropriate.<sup>118</sup>

**RECOMMENDATION 9.2**

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a new Part on data breach notification, that provides as follows:

- (1) An agency is required to notify the Privacy Commissioner and affected individuals when personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.
- (2) In determining whether the acquisition may give rise to a real risk of serious harm to any affected individual, the following factors should be taken into account:
  - (i) whether the personal information was encrypted adequately; and
  - (ii) whether the personal information was acquired in good faith by an employee or agent of the agency where the agency was

115. See also Cyberspace Law and Policy Centre, “Best practice privacy principles: suggested improvements to the ALRC’s model unified privacy principles (UPPs)”, *Submission to the Australian Government* (2008) 41.

116. For further discussion about audit and own motion investigation powers see para 10.17-10.24 and Recommendations 10.7-10.8.

117. See Recommendation 12.1.

118. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(7)(c), s 55(2)(a).

otherwise acting for a purpose permitted by the *Privacy and Personal Information Protection Act 1998* (NSW) (provided that the personal information is not used or subject to further unauthorised disclosure).

- (3) An agency is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.
- (4) Data breach notification provisions should be enforced in the same manner as an IPP under the *Privacy and Personal Information Protection Act 1998* (NSW).

## ROLE OF CRIMINAL LAW

9.45 The criminal provisions contained in PPIPA and HRIPA address a number of issues, including:

- requiring parties to attend a conciliation;<sup>119</sup>
- corrupt disclosure by public sector officials;<sup>120</sup>
- supplying personal information disclosed unlawfully;<sup>121</sup>
- disclosures by the Privacy Commissioner and Commission staff;<sup>122</sup>
- dealings with the Privacy Commissioner;<sup>123</sup>

---

119. If the Privacy Commissioner provides written notice to a public sector agency to attend conciliation, the agency must comply with the terms of the notice: *Privacy and Personal Information Protection Act 1998* (NSW) s 49(3); *Health Records and Information Privacy Act 2002* (NSW) s 46(3). This is discussed further at para 11.44.

120. *Privacy and Personal Information Protection Act 1998* (NSW) s 62; *Health Records and Information Privacy Act 2002* (NSW) s 68.

121. Where a person offers to supply personal information that they know, or reasonably ought to know, contravenes s 62 that person is guilty of an offence: *Privacy and Personal Information Protection Act 1998* (NSW) s 63; *Health Records and Information Privacy Act 2002* (NSW) s 69.

122. Where the Privacy Commissioner or a member the Privacy Commissioner's staff discloses personal information obtained in the course of his or her office in circumstances outside of discharging their functions or without the consent of relevant individuals: *Privacy and Personal Information Protection Act 1998* (NSW) s 67. This is discussed further at para 10.35.

123. Offences relating to hindering or obstructing the Privacy Commissioner or staff; failure to comply with lawful requirements of Privacy Commissioner or staff; making false statements; and where a person misrepresents that he or she is the

- failure to comply with particular orders of the ADT;<sup>124</sup> and
- intimidation, threats and misrepresentation.<sup>125</sup>

9.46 In this section we deal with the appropriateness of criminal provisions in privacy legislation and the specific issues that arise from the operation of the current criminal provisions, particularly s 62 and s 63 of PPIPA. The other issues raised above are dealt with elsewhere in this report.<sup>126</sup>

### Are criminal provisions appropriate in privacy legislation?

9.47 In CP 3 we asked whether the criminal sanction provisions in NSW privacy legislation are adequate and satisfactory.<sup>127</sup> Many submissions noted that criminal sanctions might be appropriate in certain circumstances.<sup>128</sup> We believe that the criminal sanction provisions are justified and should be retained for the following reasons.

9.48 First, the criminal provisions are aimed at “intentional” or “wilful” conduct. A strong message needs to be sent that the intentional misuse of personal information held by government is not acceptable.<sup>129</sup> The

---

Privacy Commissioner or staff: *Privacy and Personal Information Protection Act 1998* (NSW) s 68. This is discussed further at para 10.35-10.36.

124. *Health Records and Information Privacy Act 2002* (NSW) s 56. See also para 12.27.

125. Where a person uses threats, intimidation or misrepresentations to persuade or attempt to persuade an individual to: (a) refrain from making requests to access health information; (b) refrain from making complaints to the Privacy Commissioner or the Tribunal; (c) refrain from making internal review applications under the *Privacy and Personal Information Protection Act 1998* (NSW); (d) withdraw a request, complaint or application. Further, a person must not, through threats, intimidation or false representation require that another person give consent or do an act, without consent, where consent is required: *Health Records and Information Privacy Act 2002* (NSW) s 70. This is discussed further at para 10.37.

126. See Chapters 10-12.

127. NSWLRC CP 3, Issue 2.

128. Australian Privacy Foundation, *Submission, 2*; Cyberspace Law and Policy Centre, *Submission, 4*; Inner City Legal Centre, *Submission, 22-23*; NSW Department of Education and Training, *Submission, 10*. The Inner City Legal Centre “is strongly in favour of robust criminal sanctions to protect individuals against privacy violations”.

129. For example, the HIV/AIDS Legal Centre notes “in our experience, it is often a conscious decision on part of the disclosing party to release information around

existence of criminal sanctions “focus[es] the minds of public servants on compliance in a way that the other sanctions might not”.<sup>130</sup>

9.49 Secondly, the provisions catch serious conduct that contains corrupt elements.<sup>131</sup> Deterrence of misuse and corruption, given the sensitive nature of government-held information, is preferable to resolution after the fact.<sup>132</sup>

9.50 While we acknowledge that the imposition of criminal sanctions may “sit uncomfortably” with the softer methods of compliance (such as education and conciliation) taken by the Privacy Commissioner,<sup>133</sup> we believe that referral in some circumstances, which we recommend below, is effective in separating the “softer” role of the Privacy Commissioner from the enforcement of criminal sanction provisions.

### Corrupt disclosure

9.51 The “corrupt disclosure” provisions of PPIPA – s 62 and s 63 – criminalise the intentional disclosure or use of personal information by a public sector official outside the scope of his or her official functions, and conduct surrounding this disclosure: inducing or attempting to induce this disclosure, or offering to supply personal information that has been illegally disclosed.

9.52 The only case that has arisen under these provisions is the case of *DPP v Ritson*. In this case two police officers unlawfully and intentionally disclosed to a detainee that the detainee’s girlfriend had undergone

---

a person’s HIV status, rather than a question of negligence or poor privacy protection”: HIV/AIDS Legal Centre, *Submission*, 5.

130. Cyberspace Law and Policy Centre, *Submission*, 4. See also Australian Privacy Foundation, *Submission*, 2.

131. NSW Department of Education and Training, *Submission*, 10. The NSW Department of Education and Training considers the operation of the *Privacy and Personal Information Protection Act 1998* (NSW) s 62, s 63 and the *Health Records and Information Privacy Act 2002* (NSW) s 68, s 69 to be “adequate and satisfactory as a method of protecting individual privacy”.

132. HIV/AIDS Legal Centre, *Submission*, 9.

133. See Privacy NSW, *Submission*, 5; Cyberspace Law and Policy Centre, *Submission*, 4.

gender reassignment surgery 12 years previously. There was no suggestion of corruption,<sup>134</sup> but the disclosure was not in connection with the lawful exercise of their functions, as the purpose was to “embarrass” and “humiliate”.<sup>135</sup> This was found to be a “mid-range” offence under s 62,<sup>136</sup> resulting in a sentence of 125 hours of community service.<sup>137</sup>

## Issues

9.53 The following issues arise from the operation of criminal provisions:

- (1) the under-utilisation of the provisions;
- (2) the lack of remedy for complainants; and
- (3) the definition of “corrupt disclosure”.

### *Under-utilisation*

9.54 Submissions we received noted that the criminal sanction provisions contained in PPIPA are problematic because they have been utilised so infrequently.<sup>138</sup> The underutilisation of criminal provisions may be a result of: (a) the existence of alternate mechanisms to deal with corrupt conduct; and (b) general lack of awareness as to the process of instituting criminal charges.<sup>139</sup>

---

134. Transcript of Proceedings, *DPP v Ritson* (Local Court, Magistrate Bartley, 12 February 2009) 13. This decision is being appealed. **The conviction in this case was overturned on appeal, after publication: *R v Ritson* [2010] NSWDC 160.**

135. Transcript of Proceedings, *DPP v Ritson* (Local Court, Magistrate Bartley, 7 April 2009) 4.

136. Transcript of Proceedings, *DPP v Ritson* (Local Court, Magistrate Bartley, 7 April 2009) 5.

137. Transcript of Proceedings, *DPP v Ritson* (Local Court, Magistrate Bartley, 7 April 2009) 6.

138. Inner City Legal Centre, *Submission*, 23; Public Interest Advocacy Centre, *Submission*, 6. In comparison, the Business Law Committee of the Law Society believes that the criminal provisions are satisfactory and submit that the low number of cases in this area does not necessarily demonstrate a failure of these provisions: Business Law Committee of the Law Society, *Submission*, 1.

139. For example, the HIV/AIDS Legal Centre stated that it is unaware of the appropriate procedures to follow to institute criminal proceedings under either Act and submits that the provisions require clarification in reference to the process that should be followed to institute criminal charges: HIV/AIDS Legal Centre, *Submission*, 9.

9.55 Privacy NSW notes that the “State’s organisation for dealing with corrupt conduct is well established and workable”.<sup>140</sup> Corrupt conduct is generally dealt with by the Independent Commission Against Corruption (“ICAC”). However, cases have been noted where ICAC has declined to deal with matters as they have been referred to the agency in question or to Privacy NSW.<sup>141</sup> The NSW FOI/Privacy Practitioners’ Network submitted that it is unlikely, as they understand it, that an individual will be prosecuted. Rather, agencies will more likely take disciplinary action against the staff member.<sup>142</sup>

9.56 We recommend that the Privacy Commissioner and agencies should be given the power and the duty to refer any suspected offences arising under privacy legislation to NSW Police or the Director of Public Prosecutions.<sup>143</sup> This is similar to the obligation the Commonwealth Privacy Commissioner has in relation to tax file number and credit reporting offences.<sup>144</sup> It is appropriate that corrupt disclosures are referred to the authorities that have the requisite powers to investigate the conduct.<sup>145</sup> Guidelines should be issued to agencies to clarify when a referral should take place.<sup>146</sup>

---

140. Privacy NSW, *Submission*, 5.

141. For example, a university employee allegedly accessed student records to ask a student to meet him socially. Here Privacy NSW notes that “[t]his case highlights the increased privacy and corruption risks posed when people have a conflict of interest, such as where agencies engage staff members to deal with records that may relate to their own colleagues, friends or acquaintances”: Privacy NSW, *Annual Report 2002-03* (2003) 33. In another case a candidate for a position on a local council was interviewed by a selection panel and subsequently threatened by a member of the public (not involved in the recruitment process) who knew the candidate’s contact details and statements made by the candidate during the interview. The Council believed that the conduct amounted to corrupt conduct under the ICAC Act and reported it to ICAC. ICAC declined to deal with the matter as it had already been referred to the Department of Local Government and Privacy NSW. Privacy NSW notes that it was only involved in oversight of the internal review conducted by the Council: Privacy NSW, *Annual Report 2002-03* (2003) 34. See Public Interest Advocacy Centre, *Submission*, 7.

142. NSW FOI/Privacy Practitioners’ Network, *Submission*, 2.

143. This is supported by the Cyberspace Law and Policy Centre, *Submission*, 5.

144. *Privacy Act 1988* (Cth) s 49(1).

145. Investigative powers are more limited when the investigation is conducted by the Privacy Commissioner, and especially within the agency. Further concerns

**RECOMMENDATION 9.3**

The Privacy Commissioner and agencies should be under a duty to refer any suspected offences arising under privacy legislation to NSW Police or the Director of Public Prosecutions.

**RECOMMENDATION 9.4**

Once a referral has been made pursuant to Recommendation 9.3, the investigation of the Privacy Commissioner in relation to alleged criminal conduct must cease. If it is found that there is insufficient evidence to proceed with the criminal charge, the matter should be referred back to the Privacy Commissioner to complete the investigation.

*Lack of remedy for complainants*

9.57 There are no remedies for victims of unlawful disclosure in breach of s 62 of PPIPA, as knowing and intentional unlawful conduct of an official not in connection with the exercise of his or her lawful functions takes the official outside of the employment relationship. It would be inappropriate in these circumstances to impose liability on the agency as the agency has already done all that is required of it under the Act.<sup>147</sup>

9.58 It has been argued that:

it would be far preferable for agencies and organisations to be held liable for the actions of rogue employees even where they are acting *knowingly and intentionally* outside the scope of their authority. This would send a far stronger message about the need both for adequate training and security, and for effective disciplinary action against employees who act outside their authority, as well as ensuring the availability of remedies for injured complainants.<sup>148</sup>

---

in relation to investigation and internal review include witnesses' reluctance to divulge information due to potential defamation actions and the difficulties facing an officer who is reviewing the conduct of a superior: see Public Interest Advocacy Centre, *Submission*, 6; Privacy NSW, *Annual Report 2002-03* (2003) 35.

146. NSW FOI/Privacy Practitioners' Network, *Submission*, 3.

147. *Director General, Department of Education and Training v MT* (2006) 67 NSWLR 237, [51].

148. N Waters, A Paramaguru and A Johnston, *Enforcement of privacy laws – issues arising from Australian experience v. 2*, Cyberspace Law and Policy Centre, Working Paper No 3 (2007) 7-8.



9.59 While we acknowledge that this approach is persuasive, we believe that imposing liability on agencies for the unauthorised actions of their employees is both too strict a standard and contrary to established principles of agency. We have elsewhere recommended the introduction of a statutory cause of action for invasion of privacy.<sup>149</sup> We believe that, if adopted, this will alleviate the issue of a lack of a remedy for complainants in cases where unauthorised disclosure occurs.<sup>150</sup>

*Definition of corrupt disclosure*

9.60 “Corrupt disclosure” under s 62 of PPIPA and s 68 of HRIPA is not defined. Further, the text of the provision makes no mention of corruption. It provides merely that intentional disclosure or use of personal information otherwise than in connection with the lawful exercise of a public sector official’s functions is an offence. We note also that s 63 of PPIPA which is an offence consequent on s 62 does not have a corruption requirement.

9.61 It is clear from *DPP v Ritson* that s 62 of PPIPA is not limited only to “corrupt” disclosures. In the interests of clarity, we recommend that the word “corrupt” in the title of s 62 should be replaced with “criminal”. Evidence of corrupt conduct would go to the seriousness of the offence.

9.62 The requirement of corruption for the purposes of s 62(2) of PPIPA would still stand. Inducing disclosure of personal information from a public sector official is, of itself, corrupt conduct.

#### RECOMMENDATION 9.5

The title of s 62 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be modified to read “Criminal disclosure and use of personal information by public sector officials”.

149. NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009).

150. ALRC Report 108, Recommendation 50-2; Inner City Legal Centre, *Submission*, 23; Business Law Committee of the Law Society, *Submission*, 1.



10.

## **The Privacy Commissioner**

- Introduction
- Overarching functions
- Management
- Research and education
- Oversight and compliance
- Investigation and enforcement
- Legislation and policy
- Offences and liabilities

## INTRODUCTION

10.1 The functions and powers of the Privacy Commissioner are broadly outlined in Report 125, *The Offices of the Information and Privacy Commissioners* (“Report 125”).<sup>1</sup> In Report 125 we recommended that, if the Office of the Privacy Commissioner is established as a Division of the Office of the Information Commissioner (as we recommended<sup>2</sup>), the functions of the Privacy Commissioner should be divided into functions to be performed by:

- (a) both the Information and Privacy Commissioners;
- (b) the Information Commissioner;
- (c) the Privacy Commissioner; and
- (d) the Privacy Commissioner with the approval of the Information Commissioner.<sup>3</sup>

The recommendations in Report 125 are designed to improve the level of independence and oversight of the Privacy Commissioner, and ensure that the protection of privacy is afforded adequate resources.

10.2 In this chapter we consider the scope of the functions, powers and obligations of the Privacy Commissioner under privacy legislation and assess whether changes are required to improve the effectiveness of NSW privacy legislation. A major concern is the capacity of privacy legislation to bring about systemic change.<sup>4</sup> We make a number of recommendations to address this issue.

10.3 The “general functions” of the Privacy Commissioner are listed in s 36 of the *Privacy and Personal Information Act 1998* (NSW) (“PPIPA”) and s 58 of the *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”). Section 36 of PPIPA states that the Privacy Commissioner has the following functions:

- 
1. NSW Law Reform Commission, *The Offices of the Information and Privacy Commissioners*, Report 125 (2009) (“NSWLRC Report 125”).
  2. NSWLRC Report 125, Recommendations 1-4.
  3. NSWLRC Report 125, [5.2]-[5.11].
  4. See Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 99.

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

10.4 This is a general statement of functions. The functions, powers and obligations of the Privacy Commissioner are found in various places throughout privacy legislation. For the purposes of this chapter, we examine them under the following headings:

- Overarching functions.

- Management.
- Research and education.
- Oversight and compliance.
- Investigation and enforcement.
- Legislation and policy.
- Obligations and liabilities.

## OVERARCHING FUNCTIONS

10.5 In Report 125 we recommend that the Information Commissioner, in addition to the Privacy Commissioner, have the function of promoting the objects of privacy legislation.<sup>5</sup> The Information Commissioner is explicitly required to “promote the object” of the *Government Information (Public Access) Act 2009* (NSW) (the “GIPA Act”).<sup>6</sup> PPIPA does not currently contain an objects clause. The general functions of the Privacy Commissioners do not, therefore, reference the objects of privacy legislation.<sup>7</sup> We have recommended the inclusion of an objects clause in PPIPA.<sup>8</sup> The Australian Law Reform Commission (“ALRC”) has recommended that the Commonwealth Privacy Commissioner have regard to the objects of the *Privacy Act 1988* (Cth) “in the performance of his or her functions and the exercise of his or her powers”.<sup>9</sup> We believe a similar provision should be included in NSW privacy legislation. This helps to ensure that “everyone interpreting, applying and attempting to understand the Act ... has regard to the same set of objects”.<sup>10</sup>

---

5. NSWLRC Report 125, Recommendation 7.

6. *Government Information (Public Access) Act 2009* (NSW) s 17(a).

7. However, the Privacy Commissioner is required to “promote the adoption of ... the information protection principles”: *Privacy and Personal Information Protection Act 1998* (NSW) s 38(2)(a). The *Health Records and Information Privacy Act 2002* (NSW) does contain an objects clause, however the “functions of the Privacy Commissioner” does not include a reference to the objects of the Act: *Health Records and Information Privacy Act 2002* (NSW) s 58.

8. See Recommendation 1.3.

9. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”) Recommendation 46-3.

10. ALRC Report 108, vol 2, [46.46].

**RECOMMENDATION 10.1**

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to require that the Privacy Commissioner must have regard to the objects of the Act in the performance of his or her functions and the exercise of his or her powers.

**MANAGEMENT****Staff**

10.6 Privacy legislation allows for the appointment of staff of the Privacy Commissioner and delegation of Commissioner functions to “authorised” people.<sup>11</sup> However, engaging consultants or other people for the purpose of getting expert assistance requires the approval of the Minister.<sup>12</sup> The Information Commissioner has the power to engage expert assistance without the approval of the Minister.<sup>13</sup> If the model proposed in Report 125 is not adopted, we believe that the Privacy Commissioner should be able to engage consultants for the purpose of getting expert assistance without the approval of the Minister.

**RECOMMENDATION 10.2**

If the Office of the Privacy Commissioner is not established according to the model proposed in Report 125, the Privacy Commissioner should be able to engage consultants without the approval of the Minister for the purpose of getting expert assistance.

**Reporting**

10.7 The Privacy Commissioner must submit annual reports of work and activities to the Minister. The Minister must lay the report before

- 
11. *Privacy and Personal Information Protection Act 1998* (NSW) s 35, s 44. In Report 125 we recommend that if our proposed model is adopted, the Privacy Commissioner should be able to delegate functions to the staff of the “Privacy Division” within the Office of the Information Commissioner. Delegation to staff of the Office of the Information Commissioner not part of the Privacy Division can be achieved with the approval of the Information Commissioner: NSWLRC Report 125, Recommendation 11(3), Recommendation 12(4).
  12. *Privacy and Personal Information Protection Act 1998* (NSW) s 35. Under the model proposed in Report 125, expert assistance can be engaged with the approval of the Information Commissioner: NSWLRC Report 125, Recommendation 12(5).
  13. *Government Information (Information Commissioner) Act 2009* (NSW) s 16.

each House of Parliament as soon as practicable after receipt of the report.<sup>14</sup> We also recommend (later in this chapter) that the Privacy Commissioner should report annually on the operation of privacy legislation.<sup>15</sup>

## RESEARCH AND EDUCATION

10.8 The Privacy Commissioner is responsible for conducting research as well as collecting and collating information about any matter relating to the protection of personal information or health information and the privacy of individuals.<sup>16</sup> Additionally, the Privacy Commissioner is required to conduct education programs, and to disseminate information, for the purpose of promoting the protection of the privacy of individuals.<sup>17</sup> Education can help encourage a “culture of privacy protection throughout society, the economy, and government in an era of widespread adoption of new and privacy-invasive information technologies”.<sup>18</sup> It has been suggested that it may be better to allocate more of the Privacy Commissioner’s limited resources to the provision of education and advice about compliance with the Information Protection Principles (“IPPs”) and fewer resources to complaints handling.<sup>19</sup> While

---

14. *Privacy and Personal Information Protection Act 1998* (NSW) s 64.

15. See Recommendation 10.13.

16. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(f); *Health Records and Information Privacy Act 2002* (NSW) s 58(d). The *Privacy Act 1988* (Cth) s 27(1)(c) specifically requires the Commonwealth Privacy Commissioner to undertake research, and monitor developments, in data processing and computer technology. We believe that this specific requirement is encompassed by the broader requirement to conduct research into any matter relating to the protection of personal information contained in NSW legislation.

17. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(i).

18. C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd ed, 2006) 139.

19. NSW Attorney General’s Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly) (“Statutory Review of PPIPA”) [3.48]. It was recommended that “[t]he Privacy Commissioner should be encouraged to use the information collected about the sources of the Commissioner’s workload to inform the best allocation of resources. In particular, the relative importance of allocating resources to complaints handling compared with education and advice, should be reviewed”: Recommendation 1. See also Privacy NSW, *Annual Report 2001-02* (2003) 69.



we regard research and education as essential functions of the Privacy Commissioner, we would not wish to see any diminution in the resources available for complaints handling. We believe that if our recommendations in Report 125 are adopted, adequate resources will be available to enable the Privacy Commissioner to perform both functions adequately.

## OVERSIGHT AND COMPLIANCE

10.9 The Privacy Commissioner is given various functions to assist in general oversight of, and monitoring of compliance with, privacy legislation. The functions set out in privacy legislation, and recommended in this report, include:

- (1) ***Personal information digests:*** the Privacy Commissioner may, from time to time, prepare and publish a personal information digest setting out the nature and source of personal information held by public sector agencies and make this digest publicly available. The Commissioner may require a public sector agency to provide details relating to personal information held by the agency.<sup>20</sup>
- (2) ***Privacy management plans:*** PPIPA requires agencies to prepare and implement privacy management plans. These plans include information about policies, practices and procedures. A copy of this plan must be provided to the Privacy Commissioner.<sup>21</sup> The Privacy Commissioner has the function of providing assistance to public sector agencies in preparing and implementing privacy management plans.<sup>22</sup>
- (3) ***Oversight:*** the Privacy Commissioner has the power to oversee internal reviews conducted by agencies.<sup>23</sup>
- (4) ***Compliance:*** The Privacy Commissioner has the function of promoting the adoption of, and monitoring compliance with, the IPPs and Health Privacy Principles (“HPPs”).<sup>24</sup>

---

20. *Privacy and Personal Information Protection Act 1998* (NSW) s 40.

21. *Privacy and Personal Information Protection Act 1998* (NSW) s 33.

22. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(e).

23. *Privacy and Personal Information Protection Act 1998* (NSW) s 54.

- (5) **Advice:** the Privacy Commissioner has the function of providing advice on matters relating to the protection of personal information or health information and the privacy of individuals.<sup>25</sup>
- (6) **Audit powers:** to assist the Privacy Commissioner with oversight and compliance, we recommend that the Commissioner be given audit powers.<sup>26</sup>

### Personal information digests

10.10 The Commonwealth Privacy Commissioner is required to publish a personal information digest annually.<sup>27</sup> Proposed UPP 4 (Openness) requires each agency and organisation to make available Privacy Policies that clearly set out “expressed policies on the management of personal information, including how it collects, holds, uses and discloses personal information”. The ALRC concluded that this would obviate the need for a personal information digest.<sup>28</sup> The same argument could be made in relation to privacy management plans.

10.11 We agree that the adoption of UPP 4 would make the requirement to create personal information digests largely unnecessary. We note, however, that unlike the position under the *Privacy Act 1988* (Cth), the NSW Privacy Commissioner’s power is discretionary and the Commissioner is not *required* to create a personal information digest on an annual basis. The powers under the personal information digest provisions may assist the Privacy Commissioner when reporting on the operation of privacy legislation and with general responsibilities in relation to oversight and compliance, as well as legislation and policy. For that reason, we believe that the personal information digest provisions should remain in PPIPA.

---

24. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(a); *Health Records and Information Privacy Act 2002* (NSW) s 58(a).

25. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(g); *Health Records and Information Privacy Act 2002* (NSW) s 58(e).

26. See para 10.13 and Recommendation 10.5.

27. *Privacy Act 1988* (Cth) s 27(1)(g).

28. See ALRC Report 108, vol 2, [47.42].

## Privacy management plans

10.12 The adoption of the proposed UPP 4 would also make requirements in relation to privacy management plans redundant. If UPP 4 is adopted we recommend that these provisions be repealed. However, as with privacy management plans, the Privacy Commissioner should have the function of assisting public sector agencies in creating and implementing Privacy Policies under UPP 4.

---

### RECOMMENDATION 10.3

If UPP 4 is adopted in NSW, s 33 and s 36(2)(e) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be repealed.

---

### RECOMMENDATION 10.4

If UPP 4 is adopted in NSW, the Privacy Commissioner should have the function of assisting public sector agencies in creating and implementing Privacy Policies.

## Audit powers

10.13 Paragraph 27(1)(h) of the *Privacy Act 1988* (Cth) invests the Commonwealth Privacy Commissioner with the power to “conduct audits of records of personal information maintained by agencies for the purpose of ascertaining whether the records are maintained according to the Information Privacy Principles”.<sup>29</sup> The ALRC has noted, and we agree, that audit functions are an important part of the Commonwealth Privacy Commissioner’s compliance activities. The ALRC identifies such powers as a significant “proactive regulatory tool” allowing the Commissioner to monitor compliance “before, and in the absence of, evidence of non-compliance, with the aim of preventing such non-compliance occurring in the future”.<sup>30</sup> Unlike complaints handling systems, audits are not simply

---

29. There is a similar function in the *Information Privacy Act 2000* (Vic) s 58(j) which allows the Commissioner to “conduct or commission audits of records of personal information maintained by an organisation for the purpose of ascertaining whether the records are maintained according to the Information Privacy Principles or any applicable code of practice”.

30. ALRC Report 108, vol 2, [47.103].

reactive,<sup>31</sup> and may be “less confrontational”.<sup>32</sup> This power also allows the Commissioner to identify systemic issues and can assist in shaping and targeting educational materials.<sup>33</sup> The ALRC emphasises, however, that where the Commissioner reasonably believes that there has been a contravention of the privacy principles, this should be dealt with by way of own motion investigation.<sup>34</sup>

#### RECOMMENDATION 10.5

The Privacy Commissioner should be empowered to conduct or commission audits of records of personal information maintained by agencies for the purpose of ascertaining whether the records are maintained according to the IPPs or applicable codes of practice.

## INVESTIGATION AND ENFORCEMENT

10.14 Many of the Privacy Commissioner’s functions and powers relate to investigation and enforcement. Some of these functions are explored more closely in chapter 11. Broadly, the functions set out in privacy legislation, and recommended in this report, include:

- (1) *Receipt of complaints*: the Privacy Commissioner is responsible for receiving complaints multiple ways under privacy legislation.<sup>35</sup> Complaints to the Privacy Commissioner are discussed in more detail in chapter 11. However, below, we address a specific point regarding the source of the Privacy Commissioner’s complaints handling powers.<sup>36</sup>

31. See A Bendall, “The Governance of Privacy: Speak softly and carry a big stick” (Paper presented to the 2008 Australian Institute of Administrative Law Forum, Melbourne, 8 August 2008).

32. C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd ed, 2006) 135.

33. ALRC Report 108, vol 2, [47.103].

34. ALRC Report 108, vol 2, [47.105]-[47.107]. See para 10.17-10.24 and Recommendations 10.7-10.8.

35. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(k), s 45; *Health Records and Information Privacy Act 2002* (NSW) s 58(e).

36. See para 10.15-10.16.

- (2) **Investigation:** we make recommendations aimed at strengthening and clarifying the Privacy Commissioner's investigative and coercive powers in chapter 11.<sup>37</sup>
- (3) **Conciliating complaints:** the Privacy Commissioner has the function of conciliating privacy related complaints.<sup>38</sup> This is discussed in chapter 11.<sup>39</sup>
- (4) **Reports:** the Privacy Commissioner may report his or her findings and make recommendations in relation to a complaint.<sup>40</sup>
- (5) **Appearing before the Administrative Decisions Tribunal ("ADT"):** the Privacy Commissioner has the right to appear in proceedings before the ADT.<sup>41</sup>
- (6) **Data breach notification:** we recommend that the Privacy Commissioner play a pivotal role under proposed data breach notification provisions.<sup>42</sup>
- (7) **Own motion investigation:** we recommend that the Privacy Commissioner have the power to conduct own motion investigations.<sup>43</sup>
- (8) **Injunctions:** we recommend that the Privacy Commissioner have the power to apply for injunctions to address contraventions of privacy legislation.<sup>44</sup>

---

37. See para 10.3-10.27.

38. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(k), s 49.

39. See para 10.28-10.53.

40. *Privacy and Personal Information Protection Act 1998* (NSW) s 50; *Health Records and Information Privacy Act 2002* (NSW) s 47.

41. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(7). The Privacy Commissioner must also be notified of any ADT application made under the Act: *Privacy and Personal Information Protection Act 1998* (NSW) s 55(6). See also *Health Records and Information Privacy Act 2002* (NSW) s 50.

42. See para 9.27-9.44; Recommendation 9.2.

43. See para 10.17-10.24; Recommendation 10.7-10.8.

44. See para 10.25-10.26; Recommendation 10.9.

- (9) **Standing:** we recommend that the Privacy Commissioner have standing to bring proceedings in relation to the exercise of agency functions under privacy legislation.<sup>45</sup>

### Complaints handling

10.15 One of the “general functions” of the Privacy Commissioner under s 36 of PPIPA is to “receive, investigate and conciliate complaints about privacy related matters”.<sup>46</sup> In CP 3<sup>47</sup> we looked at the relationship between this broad function to look into “privacy related matters” and s 45(1) of PPIPA, which applies to the “alleged violation of, or interference with, the privacy of an individual”.<sup>48</sup> The latter uses more specific language requiring a “violation” or “interference with” privacy. We asked whether the interaction between, and the operation of, s 45, and s 36(2)(k) of PPIPA needed to be clarified.<sup>49</sup> We also queried whether these sections should be regarded as jointly regulating the Privacy Commissioner’s functions and powers with respect to complaints or as two independent sources of the Privacy Commissioner’s powers.<sup>50</sup>

10.16 The submissions that responded to this issue predominately indicate that each of the sections should be regarded as independent sources of power, and PPIPA should be clarified to achieve this.<sup>51</sup> In our view s 36(2)(k) and s 45(1) should be regarded as independent sources of power since the broader language of “privacy related matters” will enable the Privacy Commissioner to investigate a large range of issues related to privacy which cannot be easily defined.<sup>52</sup> The Privacy Commissioner can settle complaints under s 36(2)(k) informally.

---

45. See para 10.27; Recommendation 10.10.

46. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(k).

47. NSW Law Reform Commission, *Privacy Legislation in New South Wales*, Consultation Paper 3 (2008) (“NSWLRC CP 3”)

48. NSWLRC CP 3, [7.24]-[7.25].

49. NSWLRC CP 3, Issue 56(a).

50. NSWLRC CP 3, Issue 56(b).

51. Business Law Committee of the Law Society, *Submission*, 14; Cyberspace Law and Policy Centre, *Submission*, 32; Inner City Legal Centre, *Submission*, 41; NSW FOI/Privacy Practitioners’ Network, *Submission*, 11. Privacy NSW, *Submission*, 12 suggested awaiting developments in the *Privacy Act 1988* (Cth) reform process.

52. See NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009).

## RECOMMENDATION 10.6

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to make it clear that the power of the Privacy Commissioner under s 36(2)(k) “to receive, investigate and conciliate complaints about privacy related matters (including conduct to which Part 5 applies)” and the power to receive or make complaints under s 45(1) “about the alleged violation of, or interference with, the privacy of an individual” are two independent sources of power.

### Own motion investigations

10.17 The Commonwealth Privacy Commissioner may investigate an act or practice if the act or practice may be an interference with the privacy of an individual and the Commonwealth Commissioner thinks it is desirable that the act or practice be investigated.<sup>53</sup>

10.18 Current remedies following an own motion investigation are limited. Where the Commonwealth Privacy Commissioner has investigated an act or practice without a complaint being made, he or she may report to the Minister about the act or practice if (a) directed by the Minister to do so, or (b) the Commissioner thinks that the act or practice is an interference with the privacy of an individual and has not considered it appropriate to endeavour to settle the complaint or has endeavoured to settle the complaint without success.<sup>54</sup> A report to the Minister need not be made about an investigation arising out of a complaint.<sup>55</sup>

10.19 The ALRC has recommended that the Commonwealth Commissioner should be empowered to:

- issue a notice to comply following an own motion investigation where he or she determines that the agency or organisation has engaged in conduct constituting an interference with the privacy of an individual;
- prescribe in the notice specified action that must be taken by the agency or organisation to ensure compliance with the Act; and

53. *Privacy Act 1988* (Cth) s 40(2).

54. *Privacy Act 1988* (Cth) s 30(1); ALRC Report 108, vol 2, [50.3].

55. *Privacy Act 1988* (Cth) s 30(1); ALRC Report 108, vol 2, [50.4].

- commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the notice.<sup>56</sup>

10.20 The Commonwealth Government has accepted this recommendation and has noted that the procedure for dealing with an own motion investigation should be the same as for an investigation arising out of a complaint.<sup>57</sup>

10.21 Similarly, the Victorian Privacy Commissioner has the power to issue compliance notices where a breach of the IPPs is serious or systemic.<sup>58</sup> It is an offence not to comply with the notice.<sup>59</sup> The NSW Privacy Commissioner's powers under NSW privacy legislation are more limited.<sup>60</sup> Privacy NSW has recommended that the Privacy Commissioner should be given own motion investigative powers.<sup>61</sup>

#### *The Commission's view*

10.22 We recommend that the NSW Privacy Commissioner should be given the power to initiate own motion investigations for two reasons. First, it gives the Commissioner flexibility in dealing with serious issues, particularly systemic issues,<sup>62</sup> without waiting for a complaint to arise. This is consistent with the emphasis on a pre-emptive, "light-handed", cooperative approach to privacy.

10.23 Secondly, the ability to begin an own motion investigation, without a complainant, will arguably increase the willingness of individuals to report breaches of privacy without fear of recrimination or adverse consequences.

---

56. ALRC Report 108, vol 2, Recommendation 50-1.

57. Australian Government, *First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice* (2009) 97.

58. The Victorian Privacy Commissioner can issue compliance notices where the act or practice is serious or flagrant or is of a kind that has been done or engaged in by the organisation on at least 5 separate occasions within the previous 2 years: *Information Privacy Act 2000* (Vic) s 58(i), s 44(5).

59. *Information Privacy Act 2000* (Vic) s 48.

60. The Privacy Commissioner has a general power to conduct inquiries and make such investigations into privacy related matters as he or she considers appropriate: *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(l).

61. Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 106-107.

62. Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 106.



10.24 We further recommend, consistently with the ALRC recommendations, that the NSW Privacy Commissioner be able to serve compliance notices on agencies.

#### RECOMMENDATION 10.7

The Privacy Commissioner should have the power to initiate own motion investigations.

#### RECOMMENDATION 10.8

The Privacy Commissioner should be able to serve compliance notices on agencies, following an own motion investigation, that specify action that must be taken to ensure compliance with privacy legislation.

### Injunctions

10.25 Section 98 of the *Privacy Act 1988* (Cth) provides for the granting of injunctions in certain circumstances. Where a person has engaged in conduct that constituted a contravention of the *Privacy Act 1988* (Cth), the Federal Court or the Federal Magistrates Court may, on the application of the Commonwealth Commissioner or any other person, grant an injunction restraining the person from engaging in the conduct and require the person to do any act or thing.<sup>63</sup> Similarly, the Information Commissioner has the power to obtain an injunction where a person is engaging in conduct, or failing to perform an act, in contravention of an “Information Act”.<sup>64</sup>

10.26 We believe it is appropriate to have a similar power under NSW privacy legislation. This will be especially useful where the Privacy Commissioner is aware of likely future contravention and urgent intervention is required, or other informal means have failed.

#### RECOMMENDATION 10.9

The Privacy Commissioner should be able to apply to the Supreme Court to obtain an injunction where a person:

63. *Privacy Act 1988* (Cth) s 98. See also ALRC Report 108, vol 2, [50.26]-[50.34].

64. *Government Information (Information Commissioner) Act 2009* (NSW) s 28(1)-28(2).

- (1) has engaged, is engaged or is proposing to engage in any conduct that constituted, constitutes or would constitute a contravention of privacy legislation; or
- (2) has refused or failed, is refusing or failing, or is proposing to refuse or fail, to do any act or thing that the person is required to do by or under privacy legislation.

## Standing

10.27 The Information Commissioner explicitly has the power to “bring proceedings by way of judicial review in connection with the exercise of the functions of an agency under the GIPA Act”.<sup>65</sup> We believe that an equivalent power under privacy legislation would be useful for ensuring compliance with privacy legislation.

---

### RECOMMENDATION 10.10

The Privacy Commissioner should have the power to bring proceedings by way of judicial review in connection with an agency's exercise of a function under privacy legislation.

## LEGISLATION AND POLICY

10.28 There are a number of functions of the Privacy Commissioner that have a significant bearing on the scope and interpretation of privacy legislation and future policy in relation to privacy and personal information management. These include:

- (1) **Guidelines:** the Privacy Commissioner is required to “prepare and publish guidelines relating to the protection of personal information and other privacy matters”.<sup>66</sup> There are also specific references to guidelines under privacy legislation.<sup>67</sup> Additionally, we identify in this report further specific areas where the Privacy Commissioner should issue guidelines.<sup>68</sup>

---

65. *Government Information (Information Commissioner) Act 2009* (NSW) s 28(5).

66. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(b); see also *Health Records and Information Privacy Act 2002* (NSW) s 58(b).

67. *Health Records and Information Privacy Act 2002* (NSW) s 24, s 28(2), s 29, s 64, sch 1 HPPs 3, 4 and 10.

68. See Recommendations 3.1-3.3, 3.6-3.8, 5.5, 11.5.

- (2) **Privacy codes:** currently the Privacy Commissioner has functions in relation to developing and amending privacy codes of practice.<sup>69</sup> We recommend that the Privacy Commissioner should be given the additional function of approving privacy codes.<sup>70</sup> The general functions of the Privacy Commissioner should be amended to reflect this.
- (3) **Public interest directions:** the Privacy Commissioner has the power to make a written direction exempting an agency from compliance with an IPP or code with approval from the Minister. Currently the general functions of the Privacy Commissioner do not refer to public interest directions. We recommend that the Privacy Commissioner should be given the additional general function of issuing public interest directions.<sup>71</sup> The general functions of the Privacy Commissioner should be amended to reflect this.
- (4) **Special reports:** the Privacy Commissioner may, at any time, “make a special report on any matter arising in connection with the discharge of his or her functions” to Parliament.<sup>72</sup> This is discussed in further detail below.<sup>73</sup>
- (5) **Public statements:** the Privacy Commissioner currently has the power to make public statements on matters relating to the privacy of individuals generally.<sup>74</sup>
- (6) **Regulations:** currently, the Privacy Commissioner does not play a role in relation to the creation of regulations under privacy legislation. In Report 125 we recommend that the Minister consult with the Information Commissioner before creating regulations pursuant to privacy legislation.<sup>75</sup> If the model we propose in Report 125 is not adopted, the Minister

---

69. *Privacy and Personal Information Protection Act 1998* (NSW) s 31, s 36(2)(c).

70. See Recommendation 7.7.

71. See Recommendation 10.12.

72. *Privacy and Personal Information Protection Act 1998* (NSW) s 65.

73. See para 10.30-10.33.

74. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(h).

75. NSWLRC Report 125, Recommendation 10.

should be required to consult with the Privacy Commissioner instead.<sup>76</sup>

- (7) **Reporting generally:** the Privacy Commissioner currently has the general power “to prepare and publish reports and recommendations about any matter (including developments in technology) that concerns the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of individuals”.<sup>77</sup> We make further recommendations in relation to reporting on the operation of privacy legislation below.<sup>78</sup>

10.29 In Report 125, we recommended that functions relating to legislation and policy should be performed with the approval of the Information Commissioner.<sup>79</sup>

---

**RECOMMENDATION 10.11**

If Recommendations 7.7 or 7.8 are adopted, the general functions of the Privacy Commissioner should include the approval of privacy codes of practice.

---

**RECOMMENDATION 10.12**

The general functions of the Privacy Commissioner should include issuing public interest directions.

---

76. See Recommendation 7.2.

77. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(j).

78. See Recommendation 10.13.

79. NSWLRC Report 125, Recommendation 12.

## Reports to Parliament

10.30 In CP 3, we asked whether the Privacy Commissioner has the power to make a special report in relation to a complaint under s 45 of PPIPA in addition to the power to make a report under s 50, and whether legislative amendment is necessary to clarify this position.<sup>80</sup> This question was raised because s 50 expressly allows the Commissioner to make reports in relation to any findings or recommendations after a complaint has been made to them thereby, arguably, limiting the power to make a special report to Parliament.<sup>81</sup>

10.31 The apparent purpose of s 50 is to inform the complainant and other parties “materially involved” of the outcome of the complaint. If s 65 was limited by s 50 the Privacy Commissioner may be precluded from reporting to Parliament on a matter of concern to him or her, or of general public interest, arising out of the complaint.<sup>82</sup>

10.32 Submissions agreed that the Privacy Commissioner should have the power to make a special report in relation to complaints made under s 45.<sup>83</sup> Privacy NSW did not believe that clarification was necessary because it does not interpret the legislation as restricting special reports to Parliament.<sup>84</sup> However, several submissions suggested that clarification might be necessary,<sup>85</sup> especially in light of the importance of the function as a “means of ensuring government accountability and of drawing public attention to matters that raise serious and/or systemic privacy issues”.<sup>86</sup>

---

80. NSWLRC CP 3, Issue 58.

81. See NSWLRC CP 3, [7.28]-[7.30].

82. Further, the *Privacy and Personal Information Protection Act 1998* (NSW) s 46 (preliminary assessment) demonstrates that not all complaints under s 45 will be the subject of a report under s 50.

83. Cyberspace Law and Policy Centre, *Submission*, 33; Public Interest Advocacy Centre, *Submission*, 28; Privacy NSW, *Submission*, 12; NSW FOI/Privacy Practitioners’ Network, *Submission*, 11; Business Law Committee of the Law Society, *Submission*, 14.

84. Privacy NSW, *Submission*, 12.

85. Cyberspace Law and Policy Centre, *Submission*, 33; Public Interest Advocacy Centre, *Submission*, 28; NSW FOI/Privacy Practitioners’ Network, *Submission*, 11; Business Law Committee of the Law Society, *Submission*, 14.

86. Public Interest Advocacy Centre, *Submission*, 29.

*The Commission's view*

10.33 In our view there is no justification for limiting the Privacy Commissioner's power to make a special report to Parliament pursuant to s 65. However, we believe, as did Privacy NSW, that clarification is unnecessary because it is patently clear under s 65 that the Privacy Commissioner may report on *any matter* arising in connection with the discharge of his or her functions.<sup>87</sup> "Function" is defined to include "a power, authority or duty".<sup>88</sup> We believe this leaves no doubt with regard to the broad application of s 65, including in relation to complaints received under s 45.

**Reporting**

10.34 In Report 125 we recommend that the Information Commissioner be required to report annually to Parliament on the operation of privacy legislation.<sup>89</sup> This is in line with a similar obligation of the Information Commissioner under the GIPA Act.<sup>90</sup> If the proposal in Report 125 is not adopted, the Privacy Commissioner should nevertheless be required to report annually to the Minister on the operation of privacy legislation in NSW. As with annual reports, the Minister should be required to table the report in Parliament as soon as practicable after receiving it.<sup>91</sup>

**RECOMMENDATION 10.13**

If Recommendation 9 in Report 125 is not adopted, the Privacy Commissioner should be required to report annually to the Minister on the operation of privacy legislation. The Minister must table the report in each House of Parliament as soon as practicable after it has been received.

87. In fact, although it occurs infrequently, a Special Report has been issued under s 60 in addition to an investigation report under s 50, in relation to the same matter: Privacy NSW, Special Report to NSW Parliament under section 65 of the Privacy and Personal Information Protection Act 1998, *Complaint by Student A and his father against Hon John Aquilina MP, Mr Walt Secord, Mr Patrick Low*, Special Report No 2 (2002) 8.

88. *Privacy and Personal Information Protection Act 1998* (NSW) s 3.

89. NSWLRC Report 125, Recommendation 9.

90. *Government Information (Information Commissioner) Act 2009* (NSW) s 37. See NSWLRC Report 125, [5.9].

91. See para 10.7. See also *Privacy and Personal Information Protection Act 1998* (NSW) s 64.

## OFFENCES AND LIABILITIES

10.35 Privacy legislation imposes requirements that the Privacy Commissioner not disclose information outside his or her functions and also creates offences applicable to dealings with the Privacy Commissioner. Additionally, PPIPA contains a number of provisions protecting the Privacy Commissioner and others from liability in relation to complaints and investigations.<sup>92</sup> Relevant provisions include:

- (1) A requirement that the Privacy Commissioner (or member of staff) not disclose information obtained in the course of his or her functions.<sup>93</sup>
- (2) Offences relating to dealings with the Privacy Commissioner (or member of staff) with respect to functions under privacy legislation.<sup>94</sup>
- (3) Limiting the personal liability of the Privacy Commissioner (or member of staff) when acting in good faith for the purposes of executing the Act.<sup>95</sup>
- (4) Protection from liability when making a complaint under PPIPA or providing a statement, document or information to the Privacy Commissioner.<sup>96</sup>

### Intimidation and threats

10.36 Section 68 of PPIPA states that a person must not:

- without lawful excuse, wilfully obstruct, hinder or resist the Privacy Commissioner (or a member of staff) in the exercise of his or her functions;

---

92. See NSWLRC Report 125, [5.12]-[5.14].

93. This is an offence: *Privacy and Personal Information Protection Act 1998* (NSW) s 67; *Health Records and Information Privacy Act 2002* (NSW) s 68.

94. *Privacy and Personal Information Protection Act 1998* (NSW) s 68; *Health Records and Information Privacy Act 2002* (NSW) s 70. It is also an offence where a person falsely represents they are the Privacy Commissioner or member of staff.

95. *Privacy and Personal Information Protection Act 1998* (NSW) s 66.

96. *Privacy and Personal Information Protection Act 1998* (NSW) s 66A.

- without lawful excuse, refuse or wilfully fail to comply with any lawful requirement of the Privacy Commissioner (or a member of staff); or
- wilfully make any false statement to or mislead, or attempt to mislead, the Privacy Commissioner (or a member of staff) in the exercise of his or her functions.

10.37 Section 70 of HRIPA provides that a person must not, “by threat, intimidation or misrepresentation, persuade or attempt to persuade an individual” to: (a) refrain from making certain applications and complaints under HRIPA; or (b) provide consent, or act without consent as required under the Act. Similar provisions apply to the Information Commissioner where a person: “uses, causes, inflicts or procures any violence, punishment, damage, loss or disadvantage to any person” because of a complaint; assists the Information Commissioner; or provides evidence to the Information Commissioner. Further, where an employer dismisses or prejudices an employee due to the employee assisting the Information Commissioner, the employer is guilty of an offence.<sup>97</sup>

10.38 We believe similar provisions should be formulated for inclusion in PPIPA. This will be a useful safeguard to protect against practices, such as victimisation, that are fundamentally damaging to the enforcement of privacy legislation.<sup>98</sup>

---

97. *Government Information (Information Commissioner) Act 2009* (NSW) s 43(5).

98. See Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 108.



**RECOMMENDATION 10.14**

---

Privacy legislation should provide that it is an offence to use threats, intimidation or misrepresentation to persuade an individual to:

- (1) refrain from making or pursuing a complaint under privacy legislation;
- (2) refrain from making or pursuing an internal or external review application; or
- (3) withdraw a complaint or an internal or external review request.

**RECOMMENDATION 10.15**

---

Privacy legislation should provide that it is an offence to use, cause, inflict or procure any violence, punishment, damage, loss or disadvantage to any individual due to that individual:

- (1) making a complaint to the Privacy Commissioner;
- (2) assisting the Privacy Commissioner;
- (3) providing evidence to the Privacy Commissioner; or
- (4) conducting, or assisting in, an internal review.

**RECOMMENDATION 10.16**

---

Privacy legislation should provide that it is an offence for an employer to dismiss or prejudice an employee due to the employee assisting the Privacy Commissioner.



# 11. **Investigation and complaints handling**

- Introduction
- Investigation
- Complaints
- Enforceable remedies

## INTRODUCTION

11.1 This chapter begins by addressing the investigative powers of the Privacy Commissioner and considers the scope of current investigative powers and whether such powers should be extended. While these investigative powers can be used in relation to a complaint under s 45, such powers can also be used more broadly in conjunction with other functions; for example the proposed own motion investigation power or audit powers.<sup>1</sup>

11.2 This chapter then addresses complaints handling by the Privacy Commissioner and examines whether provisions addressing complaints handling require clarification or modification.

## INVESTIGATION

11.3 The Privacy Commissioner has the general function of receiving, investigating and conciliating complaints about privacy related matters<sup>2</sup> as well as conducting inquiries and investigating privacy related matters as the Commissioner considers appropriate.<sup>3</sup> The *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”) gives the Commissioner these powers:

- ***Requirement to give information:*** s 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 produce certain statements or documents.
- ***Inquiries and investigations:*** s 38(1) of PPIPA gives the Privacy Commissioner the same powers, authorities, protections and immunities as a commissioner conducting a Royal Commission.<sup>4</sup>

---

1. See Recommendation 10.5 and Recommendations 10.7-10.8.

2. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(k).

3. *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(l).

4. This is limited slightly by s 38(2) which states that s 38(1) “does not confer any function on the Privacy Commissioner that may be exercised in relation to the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the staff of the Inspector of the Independent Commission Against Corruption, Police Integrity Commission, Inspector of the

- **Personal information held by agencies:** s 40(3) of PPIPA gives the Privacy Commissioner the power to require an agency to provide details relating to the personal information held by the agency.<sup>5</sup>
- **Information about compliance arrangements:** s 42 of PPIPA gives the Privacy Commissioner the power to require an agency to provide information about how they are complying with Information Protection Principles (“IPPs”) and relevant privacy codes.<sup>6</sup> This request must be made in writing.<sup>7</sup>

11.4 The Privacy Commissioner may determine the general procedure for inquiries and investigations and is to act in an informal manner. The Commissioner is not bound by rules of evidence and is to act on the merits of the case without undue regard to technicalities.<sup>8</sup>

11.5 Sub-section 38(4) of PPIPA relates to limits on the Privacy Commissioner’s coercive powers when conducting an inquiry or investigation. It provides that 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 to compliance with the requirement and the person would not, in court proceedings, be required to comply with a similar requirement on the grounds of public interest, privilege against self-incrimination or legal professional privilege.” Further, the Privacy Commissioner cannot require any person or agency to disclose an exempt document.<sup>9</sup>

### Meaning of “person”

11.6 In CP 3, we suggested that the meaning of “person” in Part 4 of PPIPA, particularly in s 37 and s 38 may need clarification and its use in

---

Police Integrity Commission, staff of the Inspector of the Police Integrity Commission or New South Wales Crime Commissions”.

5. This is contained in the provision addressing personal information digests generally.
6. This is limited by *Privacy and Personal Information Protection Act 1998* (NSW) s 42(3).
7. *Privacy and Personal Information Protection Act 1998* (NSW) s 42(2).
8. *Privacy and Personal Information Protection Act 1998* (NSW) s 39.
9. *Privacy and Personal Information Protection Act 1998* (NSW) s 43. An exempt document is a document of a kind referred to in the *Freedom of Information Act 1989* (NSW) sch 1 cl 1 or cl 2 (ie Cabinet documents or Executive Council documents).

those sections made consistent.<sup>10</sup> Section 37 refers to “person and public sector agency”. No mention is made of a “public sector agency” under s 38(4). Sub-sections 38(5) and 38(6) also only refer to a “person”.<sup>11</sup> By contrast, s 59 and s 60 of the *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”), which are equivalent to s 37 and s 38 of PPIPA, both refer to a “person or organisation”.

*Whether “person” should be read as being restricted to “natural person”*

11.7 Submissions were divided on the question of whether the word “person” in s 37 and s 38 of PPIPA should be construed or amended to indicate clearly that it applies to a “natural person”.<sup>12</sup> The Cyberspace Law and Policy Centre submitted that the objective of these sections, which deal with the powers of the Privacy Commissioner, would be undermined by a narrow interpretation of the definition of “person” and that the Privacy Commissioner should be able to obtain relevant information from any natural or legal person, subject to the exceptions in s 38(4).<sup>13</sup>

11.8 As we noted in CP 3,<sup>14</sup> given the limited definition of “public sector agency” and having regard to the definition of “person” in s 21(1) of the *Interpretation Act 1987* (NSW), which includes a corporation and a body corporate or politic, it would be difficult to see why “person” ought to be

---

10. NSW Law Reform Commission, *Privacy Legislation in New South Wales*, Consultation Paper 3 (June 2008) (“NSWLRC CP 3”) [7.14]-[7.17], Issues 50-51.

11. These sections indicate that “[a] person is not entitled to be represented by another person at an inquiry or investigation conducted by the Privacy Commissioner except with the leave of the Privacy Commissioner” and “[t]he Privacy Commissioner may allow any person appearing before the Privacy Commissioner to have the services of an interpreter”.

12. The Cyberspace Law and Policy Centre and the Inner City Legal Centre were of the opinion that the word “person” should not be limited. The NSW Freedom of Information and Privacy Practitioners’ Network were also of the opinion that the investigative powers of the Commissioner ought not be diluted. On the other hand, the Business Law Committee of the Law Society of NSW and Privacy NSW considered, without elaboration, that PPIPA should be amended to indicate clearly that a person in s 37-38 means a “natural person”: see Cyberspace Law and Policy Centre, *Submission*, 30; Inner City Legal Centre, *Submission*, 40; Business Law Committee of the Law Society of NSW, *Submission*, 13; Privacy NSW, *Submission*, 11.

13. Cyberspace Law and Policy Centre, *Submission*, 30.

14. NSWLRC CP 3, [7.16].

given a narrow construction.<sup>15</sup> However, if this is the case, it is unclear why s 37 and s 38 refer to both a “person and public sector agency” as if the latter was not included in the definition of “person”.

11.9 Nevertheless, there are strong indications that Parliament did intend for the Privacy Commissioner’s information gathering powers to extend to private entities. Sections 37 and 38 are substantially the same as s 16 of the *Privacy Committee Act 1975* (NSW).<sup>16</sup> Under the *Privacy Committee Act 1975* (NSW), the Privacy Committee had powers not only in relation to public sector complaints but also private sector complaints.<sup>17</sup> The Privacy Committee once noted that “it may be necessary to examine other persons or bodies when investigating complaints against public authorities”.<sup>18</sup>

11.10 The same reasoning applies in relation to a narrow interpretation of the term “person” in s 37 and s 38 of PPIPA. To exclude “legal persons” from the definition of “person” does not take into account that the

- 
15. It is accepted that the Crown is a body politic, and thus that the Crown in all its particular rights (such as the Crown in right of a State) is still an indivisible body politic, (*Magdalen College Case* (1615) 11 Co Rep 66b, 70a; *Melbourne Harbour Trust Commissioners v Colonial Sugar Refining Company Ltd* (1925) 36 CLR 230, 279) and thus that the Crown in all its particular rights (such as the Crown in right of a State) is still an indivisible body politic. A council is thus a body politic (*Local Government Act 1990* (NSW) s 220(1)), as is any Commonwealth instrumentality or agency (*Corporations Act 2000* (Cth) s 5A(1)). It has been held that “the expression ‘body politic’... indicates...a body created for some public purpose” (*Melbourne Harbour Trust Commissioners v Colonial Sugar Refining Company Ltd* (1925) 36 CLR 230, 279) and that the Police Service of NSW is a body politic (*Workcover Authority of NSW (Inspector Keelty) v The Crown in Right of the State of NSW (Police Service of NSW)* [2000] NSWIRComm 234).
  16. When the *Privacy and Personal Information Protection Act 1998* (NSW) came into effect, it replaced the Privacy Committee with the appointment of a Privacy Commissioner and Privacy Advisory Committee.
  17. Sub-section 16(1) conferred on the Committee the power to “require any person (a) to give any statement of information; (b) to produce any document or thing; or (c) to give a copy of any document”.
  18. In response to the unsuccessful Privacy and Data Protection Bill 1994 (NSW) which proposed limiting the information gathering powers to public authorities and officials: NSW Privacy Committee, *Submission to the Select Committee on the Privacy and Data Protection Bill 1994* (July 1994) 53.

Privacy Commissioner may need to examine corporate bodies when investigating complaints against public sector agencies.<sup>19</sup>

11.11 It is important to note that while the core of PPIPA is a series of IPPs applicable only to the public sector, its objectives, and the functions of the Privacy Commissioner, are also to promote privacy protection generally.<sup>20</sup> In order to discharge these functions, it is essential that the Privacy Commissioner be equipped with information gathering powers not only in relation to public sector agencies but also corporate entities.

11.12 In our view, the term “person” in s 37 and s 38 should include not only natural but “legal” persons. In order to clarify this position, we recommend, subject to the discussion on s 38(4) below, that where the phrase “person or public sector agency” appears in s 37 and s 38, the words “or public sector agency” be deleted, such that the term “person” can be given its ordinary interpretation under the *Interpretation Act 1987* (NSW). This interpretation would be aided by amending PPIPA to define “person”, without limiting the definition of “person” in the *Interpretation Act 1987* (NSW), to include a public sector agency. This is similar to approach under the *Government Information (Public Access) Act 2009* (NSW) (the “GIPA Act”).<sup>21</sup>

11.13 This terminology would be consistent with the powers of the newly-created NSW Information Commissioner,<sup>22</sup> the way that the

---

19. This is particularly so in light of the Commission’s recommendation to extend contractually the NSW privacy regime to government contractors: Recommendation 2.5.

20. The general functions of the Privacy Commissioner include not only functions relating specifically to the IPPs contained in PPIPA or public sector agencies, but also includes the investigation and conciliation of complaints about privacy related matters, conducting inquiries into privacy related matters as the Privacy Commissioner thinks appropriate, as well as conducting research, giving advice and disseminating information on “protection of personal information and other privacy matters” generally: see *Privacy and Personal Information Protection Act 1998* (NSW) s 36.

21. See *Government Information (Public Access) Act 2009* (NSW) sch 4 cl 1 where “person” is defined to include “an agency, the government of another jurisdiction (including a jurisdiction outside Australia) and an agency of the government of another jurisdiction”. This definition does not limit the definition of “person” in the *Interpretation Act 1987* (NSW), which includes an individual, a corporation and a body corporate or politic.

22. See *Government Information (Information Commissioner) Act 2009* (NSW) s 27(3) definition of “coercive investigative power”.



powers of the Commonwealth Privacy Commissioner are framed,<sup>23</sup> and similar provisions in other State jurisdictions.<sup>24</sup>

*Whether a public sector agency can claim privilege against a Privacy Commissioner's coercive powers in an inquiry or investigation*

11.14 The omission of a reference to “public sector agency” in s 38(4) of PPIPA would suggest that the Parliamentary intention was that the exemption from a requirement to give or produce certain statements or documents in an inquiry or investigation being conducted by the Privacy Commissioner on the grounds of public interest, self-incrimination or legal professional privilege does not apply to public sector agencies.

11.15 We noted in CP 3 that it is difficult to see why 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.<sup>25</sup> 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”.<sup>26</sup>

11.16 It is possible that, since s 38 was adopted from s 16 of the *Privacy Committee Act 1975* (NSW), which refers only to “persons”, it was omitted through oversight. Further, the High Court has held that, as legal professional privilege is “not merely a rule of substantive law”, but rather “an important common law immunity”, it could only be abrogated expressly or by necessary implication.<sup>27</sup> In the absence of an express

---

23. *Privacy Act 1988* (Cth) s 43(3), s 44-46. The power to obtain information and documents is subject to s 69-70. It is an offence not to comply with the Commissioner's directions: *Privacy Act 1988* (Cth) s 46(2), s 65-66.

24. See *Information Privacy Act 2009* (Qld) s 116, which relates to the powers of the Information Commissioner on external review and refers to requiring “a person” to give or produce information; *Information Privacy Act 2000* (Vic) s 45, which refers to the powers of the privacy commissioner to require “a person” to give information or produce a document.

25. NSWLRC CP 3, [7.15].

26. NSWLRC CP 3, [7.17].

27. *Daniels Corporation International Pty Ltd v Australian Competition and Consumer Commission* (2002) 213 CLR 543, [11]. In relation to the privilege against self-incrimination see *Environment Protection Authority v Caltex Refining Co Pty Ltd*

indication in PPIPA that s 38(4) does not apply to public sector agencies, Parliament may not have intended such an abrogation.

11.17 Few stakeholders considered the question whether both s 37 and s 38(4) of PPIPA apply to a “person or public sector agency”, but those that did were, for the same reasons expressed in CP 3, in favour of making such an amendment.<sup>28</sup>

11.18 Regardless of whether or not the abrogation of these privileges in the context of an inquiry or investigation by the Privacy Commissioner was intended, there have been developments at both the Commonwealth as well as State and Territory levels that need to be noted. The Australian Law Reform Commission (“ALRC”) considered the impediments presented by misuse of claims of legal profession privilege to federal investigations and concluded that legal professional privilege is a doctrine of fundamental importance in the common law.<sup>29</sup> The default position in relation to coercive information gathering powers in federal investigations is that legal professional privilege applies in the absence of express abrogation.<sup>30</sup> However, the ALRC recognised that the privilege may be modified or abrogated by legislation if Parliament chooses to give higher priority to the interests of investigatory agencies in accessing information.

11.19 Some jurisdictions have recognised a public interest in allowing the interests of investigatory agencies in accessing information to prevail over the interests served by maintaining privilege in privacy and freedom of information contexts.<sup>31</sup> Section 113 of the *Information Privacy Act 2009* (Qld) provides that in the context of an external review application, the Queensland Information Commissioner is entitled to full and free access to the documents of the agency or Minister concerned, including

---

(1993) 178 CLR 477, 509; in relation to classes of documents subject to the public interest immunity see *Commonwealth v Northern Land Council* (1993) 176 CLR 604, 618.

28. See Cyberspace Law and Policy Centre, *Submission*, 30; Inner City Legal Centre, *Submission*, 40; Business Law Committee of the Law Society of NSW, *Submission*, 64; Privacy NSW, *Submission*, 11.

29. Australian Law Reform Commission, *Privilege in Perspective: Client Legal Privilege in Federal Investigations*, Report 107 (2008) (“ALRC Report 107”).

30. ALRC Report 107, Recommendations 5-2 and 5-3, 29.

31. See *Information Privacy Act 2009* (Qld); *Ombudsman Act 1978* (Tas); and *Personal Information Protection Act 2004* (Tas).

documents protected by legal professional privilege.<sup>32</sup> The Explanatory Memorandum explains that “[t]he abrogation of the right to claim legal professional privilege is justified as being necessary to ensure the Information Commissioner has the ability to properly consider and determine external reviews”.<sup>33</sup>

11.20 However, the Act places obligations on the Information Commissioner and the Commissioner’s staff to ensure such information is protected from disclosure (other than to specified persons) and that documents are returned at the end of an external review. Additionally, under s 120 the Information Commissioner must make such directions as are considered necessary to avoid disclosure to an access participant.<sup>34</sup>

11.21 In Tasmania, the Crown is not entitled to prevent or obstruct records from being produced, or evidence from being given, for the purpose of an investigation by the Ombudsman notwithstanding that it would be so entitled if the investigation were a legal proceeding held before a court.<sup>35</sup> Further, a person is not excused from giving information, or producing a record or answering a question, when required to do so by the Privacy Commissioner on the ground that to do so would disclose legal advice furnished to a government department or public authority.<sup>36</sup>

11.22 NSW has already made a step in the direction of abrogation in defining the coercive powers of the Information Commissioner. In s 27(1) of the *Government Information (Information Commissioner) Act 2009* (NSW), the Commissioner must set aside any requirement imposed under a coercive investigative power if it appears to the Commissioner that any

---

32. See also *Information Privacy Act 2009* (Qld) s 119(2), which provides that legal professional privilege does not apply to the production of documents or the giving of evidence by a member of an agency or Minister for the purposes of external review.

33. Explanatory Notes, *Information Privacy Bill 2009* (Qld) 5.

34. It is also an offence for the Information Commissioner or a staff member to disclose information obtained in performance of functions under the Act: *Information Privacy Act 2009* (Qld) s 188.

35. See *Ombudsman Act 1978* (Tas) s 24(2). The *Personal Information Protection Act 2004* (Tas) s 21(1) provides that if the Ombudsman decides to deal with a privacy complaint, the Ombudsman is to conduct any investigations in relation to the complaint in accordance with the *Ombudsman Act 1978* (Tas) div 3 pt 3.

36. See *Ombudsman Act 1978* (Tas) s 24(3).

person has a ground of privilege unless, under s 27(1)(a) “the privilege is a privilege of an agency”.

11.23 Further consideration needs to be given before abrogating legal professional privilege in relation to investigations of the Privacy Commissioner, where different considerations may apply. The Commonwealth government has not sought to clarify the operation of privilege under the Commonwealth privacy regime. In its submission to the ALRC review on privilege, the Office of the Commonwealth Privacy Commissioner took the view that a claim for legal professional privilege falls within the “reasonable excuse” defence for not complying with a coercive information gathering power under the *Privacy Act 1988* (Cth), and there was no need to clarify the application of the privilege to its powers under the Act.<sup>37</sup>

11.24 There is not yet a compelling reason to abrogate the privileges of public sector agencies in the context of the Privacy Commissioner’s investigations and inquiries, particularly where the Office of the Commonwealth Privacy Commissioner has not had reason to consider the use or abuse of legal professional privilege to be an impediment to its investigations. Thus, we believe that there is no current need for s 38(4) to exclude public sector agencies. However, if such a need does arise, we are of the view that any abrogation needs to be accompanied by adequate measures to ensure such information is protected. While s 67 of PPIPA makes it an offence for the Privacy Commissioner or a member of his or her staff to disclose personal information obtained in the course of his or her office, other safeguards such as those found in s 120 of the *Information Privacy Act 2009* (Qld) may be warranted.

11.25 Accordingly, we are of the view that both s 37 and s 38(4) of PPIPA should apply to “any persons” or “the person concerned”.

#### *Cabinet or Executive Council documents*

11.26 Section 43 of PPIPA also states that neither PPIPA nor HRIPA authorises the Privacy Commissioner to require “any person or public sector agency” to disclose an “exempt document” under cl 1 or cl 2 of sch 1 to the *Freedom of Information Act 1989* (NSW).<sup>38</sup> Given the powerful

---

37. ALRC Report 107, [5.64], [5.70]. See *Privacy Act 1988* (Cth) s 66(1B).

38. Exempt documents refers to Cabinet documents or Executive Council documents.

public interest in ensuring the confidentiality of such documents,<sup>39</sup> the reference to “any person or public sector agency” in s 43 will also have to be replaced with “any persons” in order to make it clear that neither natural nor legal persons can be forced to disclose Cabinet or Executive Council documents under PPIPA or HRIPA.

#### RECOMMENDATION 11.1

Sub-sections 37(1), 37(2)(a), 37(2)(b) and 43(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to refer to “any person” rather than “any person or public sector agency”.

#### RECOMMENDATION 11.2

The *Privacy and Personal Information Protection Act 1998* (NSW) should, without limiting the definition of “person” in the *Interpretation Act 1987* (NSW), state that “person” includes a public sector agency.

### Extension of investigative powers

#### *Entry on premises*

11.27 The Information Commissioner and the Ombudsman have the power to enter and inspect premises occupied or used by a public authority and inspect any document or thing on the premises.<sup>40</sup> A similar power is given to the Commonwealth Privacy Commissioner.<sup>41</sup> The Privacy Commissioner is given broad investigative powers as well as accompanying coercive powers, recognising the Commissioner’s important oversight role. Extending these powers to include entering premises where required for investigation is consistent with this role, and in line with the powers of similar statutory office holders.

#### RECOMMENDATION 11.3

The Privacy Commissioner should be given the power to enter and inspect premises occupied by a public sector agency and inspect any document or thing on the premises.

39. *Commonwealth v Northern Land Council* (1993) 176 CLR 604, 618.

40. *Ombudsman Act 1974* (NSW) s 20; *Government Information (Information Commissioner) Act 2009* (NSW) s 26.

41. *Privacy Act 1988* (Cth) s 68.

## COMPLAINTS

11.28 Sub-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”.<sup>42</sup> The complaint must be made within six months from the time the complainant first became aware of the conduct or matter the subject of the complaint; or later if permitted by the Privacy Commissioner.<sup>43</sup>

### Third party complaints

11.29 Application of s 45 does not appear to be limited to the person involved. However, a *Privacy NSW Complaints Protocol* was issued indicating that the Privacy Commissioner had received legal advice to the effect that this section is limited to an individual whose privacy had been violated and those acting behalf of that individual.<sup>44</sup>

11.30 In CP 3 we asked if s 45(1) should 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.<sup>45</sup> Submissions generally supported clarifying s 45(1) to confirm that third parties can also make complaints.<sup>46</sup> The Cyberspace Law and Policy Centre notes that the

---

42. A complaint may be in writing or verbal, the Privacy Commissioner may require that the complaint be made in writing. The Commissioner may also require that information about a complaint to be provided in a particular manner or form, and may require the complaint be verified by statutory declaration: *Privacy and Personal Information Protection Act 1998* (NSW) s 45(3), s 45(4).

43. *Privacy and Personal Information Protection Act 1998* (NSW) s 45(5).

44. Privacy NSW Complaints Protocol (issued 22 July 2002, revised July 2006) [2.2.2]. Note that this Protocol has been removed from the Privacy NSW website for revision (as at 12 January 2010). This issue was also noted in Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 102.

45. NSWLRC CP 3, Issue 53.

46. Cyberspace Law and Policy Centre, *Submission*, 31; Australian Privacy Foundation, *Submission*, 13; Public Interest Advocacy Centre, *Submission*, 28; Inner City Legal Centre, *Submission*, 41; NSW Commission for Children and Young People, *Submission to the Australian Law Reform Commission Review of Privacy Issues Paper* (2007) 7. NSW FOI/Privacy Practitioners’ Network, *Submission*, 10-11 did not agree. Privacy NSW, *Submission*, 11; Business Law Committee of the Law Society of NSW, *Submission*, 13; NSW Department of

“nature of many privacy breaches is such that the particular individuals affected may not even be aware of the breach, and so the scheme relies on ‘whistleblowers’ to bring a complaint”.<sup>47</sup> There may be many reasons why an individual may not want to bring a complaint, for example, power imbalance, fear of adverse action from the agency, low income or other disadvantage. Provision should therefore be in place for third parties to raise “public interest” complaints.<sup>48</sup> The Inner City Legal Centre points out that “a situation should not be able to arise whereby a complaint is prevented by the fact that the person whose privacy has been violated is unaware of the violation or does not themselves make a complaint”.<sup>49</sup>

11.31 In contrast, the NSW FOI/Privacy Practitioners’ Network submits that while a third party could lodge a complaint on behalf of another, “it would be inappropriate for individuals to make a complaint when they have no real interest in the matter or merely wish to be a serial complainant”.<sup>50</sup> The Network further notes that this is a problem that is already occurring in the context of the *Ombudsman Act 1974* (NSW).<sup>51</sup>

11.32 Former Privacy Commissioner, Chris Puplick, raised the issue of third party complaints in a Special Report to Parliament. It was suggested that the Privacy Commissioner did not have jurisdiction to investigate complaints from third parties and as a result, the investigation into a complaint was discontinued:

I regard this as an unsatisfactory situation, since the ability to raise questions of privacy should not, in my view, be limited to only those who have suffered personal damage, harm or embarrassment. There are many circumstances in which complaints might be brought by third parties including alleged violations of privacy in the workplace or in matters affecting children and individuals under the care of others. There are also circumstances where a third party acting in the capacity of a whistleblower might wish to bring matters to my attention which do not necessarily affect him or her, such as the misuse of personal information contained in a database. I do not believe the Parliament intended that I would be unable to deal with such matters and I am inviting the Parliament, by way of a

---

Corrective Services, *Submission*, 6 note that third parties should be able to act on behalf of individuals.

47. Cyberspace Law and Policy Centre, *Submission*, 31.

48. Cyberspace Law and Policy Centre, *Submission*, 31.

49. Inner City Legal Centre, *Submission*, 41.

50. NSW FOI/Privacy Practitioners’ Network, *Submission*, 10-11.

51. NSW FOI/Privacy Practitioners’ Network, *Submission*, 11.

Recommendation in this Report, to consider this matter and examine possible amendments to the PPIP Act accordingly.<sup>52</sup>

11.33 We agree that third parties should be able to make complaints to the Privacy Commissioner under s 45(1) of PPIPA. Limiting the application of s 45(1) creates a “significant accountability gap”.<sup>53</sup> We believe that PPIPA gives the Privacy Commissioner a broad power to receive and investigate complaints and this also appears evident in the language of s 45.<sup>54</sup> However, it is also clear that this is not the way in which this provision has been interpreted, and therefore amendment may be required to make this explicit.

#### RECOMMENDATION 11.4

Sub-section 45(1) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be reworded to clarify that it is not limited to an individual whose privacy has been violated, or a person acting on behalf of that individual.

#### Violation or interference with privacy

11.34 PPIPA does not provide guidance as to what matters the Privacy Commissioner may take into account in assessing and dealing with complaints under s 45(1). More information is provided in the *Privacy NSW Complaints Protocol*.<sup>55</sup>

11.35 On a Commonwealth level, individuals have the right to make a complaint to the Commonwealth Privacy Commissioner “about an act or

52. Privacy NSW, Special Report to NSW Parliament under section 65 of the Privacy and Personal Information Protection Act 1998, *Complaint by Student A and his father against Hon John Aquilina MP, Mr Walt Secord, Mr Patrick Low*, Special Report No 2 (2002) 19.

53. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 102. Note that under internal review provisions, “person aggrieved” is not limited to the person who is the subject of the personal information at issue: *KO v Commissioner of Police, NSW Police* [2004] NSWADT 3.

54. And also the language used under the “general functions” of the Privacy Commissioner: *Privacy and Personal Information Protection Act 1998* (NSW) s 36.

55. *Privacy NSW Complaints Protocol* (issued 22 July 2002, revised July 2006). Note that this Protocol has been removed from the Privacy NSW website for revision (as at 12 January 2010).



practice that may be an interference with the privacy of the individual”.<sup>56</sup> “Interference with privacy” is more limited in this context, and is defined in the Act according to who engages in the act or practice or the nature of the act or practice itself.<sup>57</sup>

11.36 In CP 3 we asked whether the meaning of “violation of” and “interference with” an individual’s privacy in s 45(1) of PPIPA should be clarified and whether legislation should 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”.<sup>58</sup> Some submissions supported clarification of the meaning of “violation of” or “interference with” an individual’s privacy.<sup>59</sup> Others argued that legislative clarification would make the provision too prescriptive,<sup>60</sup> noting that the meaning of these terms should be developed on a case-by-case basis.<sup>61</sup> Clarification could limit the ability of the Privacy Commissioner to investigate complaints and make the provision inflexible and incapable of accommodating changing circumstances such as technological advancements.<sup>62</sup>

11.37 It is clear that the terms “violation of” and “interferences with” privacy could include breach of the IPPs, but also includes matters within the broader notion of privacy.<sup>63</sup> We do not believe that it would be

---

56. *Privacy Act 1988* (Cth) s 36(1); Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008) (“ALRC Report 108”), vol 2, [49.3].

57. See *Privacy Act 1988* (Cth) s 13, s 13A. For example, for an agency, an act or practice which breaches an IPP constitutes an interference with privacy.

58. NSWLRC CP 3, Issues 54-55.

59. Privacy NSW, *Submission*, 12; Cyberspace Law and Policy Centre, *Submission*, 32; Australian Privacy Foundation, *Submission*, 13; Business Law Committee of the Law Society, *Submission*, 13.

60. NSW FOI/Privacy Practitioners’ Network, *Submission*, 11.

61. Inner City Legal Centre, *Submission*, 41.

62. NSW FOI/Privacy Practitioners’ Network, *Submission*, 11.

63. Section 45(2) continues by saying that the subject matter of a complaint *may* be related to conduct to which the internal review process applies. This suggests that a complaint may also be made about other privacy related matters. This reading is supported by s 46(2), which says *if* the subject-matter of the complaint relates to conduct to which the internal review process applies, the Privacy Commissioner must ensure the complainant is aware that the process exists and the remedies that might be available.

appropriate to define these terms in the legislation. To do so would not allow for flexibility in application. The Privacy Commissioner should continue to issue guidelines to indicate what he or she will take into account when determining whether to deal with a complaint pursuant to s 45.

#### RECOMMENDATION 11.5

The Privacy Commissioner should issue guidelines to indicate what he or she will take into account when determining whether to deal with a complaint under privacy legislation.

#### Preliminary assessment

11.38 The Privacy Commissioner can undertake a preliminary assessment in order to determine whether to deal with a complaint under Part 4, Division 3 of PPIPA.<sup>64</sup> The Privacy Commissioner can decide not to deal with a complaint if he or she is satisfied that the complaint is frivolous, vexatious, or lacking in substance; not in good faith; trivial; relates to a matter permitted or required under law; an alternate satisfactory and readily available means of redress is available; or an internal review application would be more appropriate.<sup>65</sup> A complainant may also withdraw a complaint.<sup>66</sup>

11.39 Similarly, the Commonwealth Privacy Commissioner has the discretion not to investigate or to defer investigation in certain circumstances.<sup>67</sup> The ALRC has indicated a number of ways in which this

64. *Privacy and Personal Information Protection Act 1998* (NSW) s 46(1). If the subject-matter of the complaint relates to conduct to which the internal review process applies the Privacy Commissioner must ensure the complainant is aware that the process exists and the remedies that might be available: s 46(2).

65. *Privacy and Personal Information Protection Act 1998* (NSW) s 46(3). See also *Health Records and Information Privacy Act 2002* (NSW) s 43.

66. *Privacy and Personal Information Protection Act 1998* (NSW) s 46(6).

67. He or she is satisfied that the practice is not an interference with privacy; more than 12 months have passed since the complainant became aware of the conduct; the complaint is frivolous, vexatious, misconceived or lacking in substance; the conduct is, or has been, adequately dealt with under another law or another law can provide a more appropriate remedy for the relevant conduct; the respondent has dealt, or is dealing with the complaint adequately or has not yet had an adequate opportunity to deal with the complaint; or the respondent has applied for a public interest determination and the Commonwealth

discretion should be broadened. This includes, where the complainant is unresponsive;<sup>68</sup> where an investigation is not warranted having regard to all the circumstances;<sup>69</sup> and where the complaint is being, or would more suitably be, handled by an external dispute resolution scheme recognised by the Commonwealth Privacy Commissioner.<sup>70</sup> We believe some aspects of this are encompassed by the NSW Privacy Commissioner's existing discretion. We agree, however, that where a complainant has not responded to the Commissioner for a specified period following a request for a response in relation to the complaint, the Privacy Commissioner should be able to elect not to deal with the complaint.

#### RECOMMENDATION 11.6

The Privacy Commissioner should be able to decide not to deal with a complaint if the complainant has not responded to the Commissioner for a specified period following a request by the Commissioner for a response in relation to the complaint.

#### Referral

11.40 The Privacy Commissioner can refer a complaint under Part 4, Division 3 of PPIPA to any person or body considered appropriate in the circumstances (the "relevant authority") for investigation or other action. The Privacy Commissioner may communicate information it has obtained in relation to the complaint to the relevant authority. Referral can only be made after consultation with the complainant and the relevant authority. Their views must be taken into consideration.<sup>71</sup>

---

Commissioner is satisfied that the interests of the person affected by the conduct would not be unreasonably prejudiced if the investigation was deferred until the application has been disposed of: *Privacy Act 1988* (Cth) s 41.

68. That is, where the complainant has not responded to the Commonwealth Privacy Commissioner for a specified period following a request by the Commissioner for a response in relation to the complaint: ALRC Report 108, vol 2, Recommendation 49-1.

69. ALRC Report 108, vol 2, Recommendation 49-1.

70. ALRC Report 108, vol 2, Recommendation 49-2.

71. *Privacy and Personal Information Protection Act 1998* (NSW) s 47. See also *Health Records and Information Privacy Act 2002* (NSW) s 65-67.

## Dealing with a complaint

11.41 The discussion above reveals multiple bases upon which the Privacy Commissioner may not be required to deal with a complaint, including:

- the complaint is not a complaint about the “alleged violation of, or interference with, the privacy of an individual”;<sup>72</sup>
- the complaint has not been made within the required time, and the Privacy Commissioner does not permit an extension;<sup>73</sup>
- the complaint has been withdrawn;<sup>74</sup>
- the Commissioner has conducted a preliminary assessment and has decided not to deal with the complaint due to some or all of the matters listed in s 46(3);<sup>75</sup> or
- the complaint has been referred to a relevant authority pursuant to s 47.<sup>76</sup>

11.42 If the Privacy Commissioner decides to deal with a complaint they may make such inquiries and investigations in relation to the complaint as they consider appropriate.<sup>77</sup> If the Privacy Commissioner does not elect to deal with the complaint, the Commissioner must advise the complainant and provide reasons for the denial.<sup>78</sup> If the subject matter of the complaint relates to conduct to which internal review provisions apply, the Privacy Commissioner must inform the complainant of the review process and remedial action that may be available if the complainant makes an internal review application.<sup>79</sup>

---

72. *Privacy and Personal Information Protection Act 1998* (NSW) s 45(1).

73. *Privacy and Personal Information Protection Act 1998* (NSW) s 45(5).

74. *Privacy and Personal Information Protection Act 1998* (NSW) s 45(6).

75. See para 11.38-11.39.

76. See para 11.40.

77. *Privacy and Personal Information Protection Act 1998* (NSW) s 48(1). Under the *Health Records and Information Privacy Act 2002* (NSW) s 44 the Privacy Commissioner must also determine whether there is a prima facie case and, if satisfied that a prima facie case exists, proceed to “deal” with a complaint under s 45.

78. *Privacy and Personal Information Protection Act 1998* (NSW) s 48(2). See also *Health Records and Information Privacy Act 2002* (NSW) s 43(3).

79. *Privacy and Personal Information Protection Act 1998* (NSW) s 46(2).

11.43 Under s 51 of PPIPA, even if the Privacy Commissioner declines to deal with a complaint, or decides to refer the complaint to a relevant authority, he or she may “conduct an inquiry or investigation into any general issues or matters raised in connection with the complaint”.<sup>80</sup> In CP 3 we asked whether s 51 required clarification with respect to the Privacy Commissioner’s power to conduct an inquiry or investigation into any general issue raised by a withdrawn complaint.<sup>81</sup> The majority of submissions that responded to this issue argued that s 51 should also apply to withdrawn complaints.<sup>82</sup> Submissions noted that this could help address systemic issues,<sup>83</sup> act as a deterrent<sup>84</sup> and noted “the public interest underlying this provision should not depend on whether a complaint is withdrawn or not”.<sup>85</sup> We agree that the Privacy Commissioner should have the discretion to conduct an inquiry or investigation into any general issue raised by a withdrawn complaint. This will demonstrate that the focus is not only on the individual complainant but also investigation and resolution of systemic privacy issues.

#### RECOMMENDATION 11.7

The Privacy Commissioner should have the power to conduct an inquiry or investigation into any general issue raised by a withdrawn complaint.

#### Conciliation

11.44 The Privacy Commissioner must endeavour to resolve by conciliation complaints under Part 4, Division 3 of PPIPA.<sup>86</sup> The Privacy

80. *Privacy and Personal Information Protection Act 1998* (NSW) s 51.

81. NSWLRC CP 3, Issue 57.

82. Privacy NSW, *Submission*, 12; Cyberspace Law and Policy Centre, *Submission*, 32; Public Interest Advocacy Centre, *Submission*, 28; Inner City Legal Centre, *Submission*, 42; NSW FOI/Privacy Practitioners’ Network, *Submission*, p 11. Business Law Committee of the Law Society of NSW, *Submission*, 14, did not agree.

83. Public Interest Advocacy Centre, *Submission*, 28; NSW FOI/Privacy Practitioners’ Network, *Submission*, 11.

84. Inner City Legal Centre Centre, *Submission*, 42.

85. Cyberspace Law and Policy Centre, *Submission*, 32.

86. *Privacy and Personal Information Protection Act 1998* (NSW) s 49(1). Compare the *Health Records and Information Privacy Act 2002* (NSW) s 46 where the Privacy Commissioner *may* endeavour to resolve the complaint by conciliation. Note

Commissioner may by written notice request the complainant and the respondent to appear before him or her in conciliation proceedings. If the respondent is a public sector agency it must comply with the terms of the notice under s 49(2). Failure to do so is an offence under PPIPA. Parties to conciliation proceedings can only be represented by another person by leave of the Privacy Commissioner.<sup>87</sup>

11.45 In contrast, at the Commonwealth level, after an investigation, a complaint can be resolved through conciliation or through a determination of the Commonwealth Privacy Commissioner.<sup>88</sup> The Commonwealth Privacy Commissioner is only required to conciliate complaints where he or she considers it appropriate to do so.<sup>89</sup> However, the precise process of complaints handling is unclear under the Commonwealth legislation. The ALRC has recommended that express provisions dealing with the conciliation process be included in the *Privacy Act 1988* (Cth). These provisions would provide that if, after accepting a complaint, the Commonwealth Privacy Commissioner considers it reasonably possible that it can be conciliated successfully, he or she must make reasonable attempts at conciliation.<sup>90</sup> The ALRC further recommended that where there have been reasonable attempts to conciliate a complaint, and the Commonwealth Privacy Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify both parties that conciliation has failed.<sup>91</sup> We believe that it would be useful to include a

---

that the Privacy Commissioner will determine the procedures for conciliation: *Privacy and Personal Information Protection Act 1998* (NSW) s 49(5). See also *Health Records and Information Privacy Act 2002* (NSW) s 46(5).

87. *Privacy and Personal Information Protection Act 1998* (NSW) s 49. See also *Health Records and Information Privacy Act 2002* (NSW) s 46.

88. ALRC Report 108, vol 2, [49.39].

89. *Privacy Act 1988* (Cth) s 27(1)(a), s 27(1)(ab); ALRC, Report 108, vol 2, [49.40].

90. See ALRC Report 108, vol 2, Recommendation 49-5.

91. See ALRC Report 108, vol 2, Recommendation 49-5. The ALRC further recommends that the *Privacy Act 1988* (Cth) be amended to empower the Commonwealth Privacy Commissioner to compel parties to a complaint and any other relevant person to attend a compulsory conference (previously limited to agencies): See ALRC Report 108, vol 2, Recommendation 49-11, [49.121]. The ALRC also recommends that the Commonwealth Privacy Commissioner be empowered to direct that a hearing for a determination be conducted without oral submissions from parties if he or she is satisfied that the matter could be

similar a provision in PPIPA. This will trigger Administrative Decisions Tribunal (“ADT”) external review processes, as recommended in chapter 9,<sup>92</sup> and establish applicable time limits for appeal to the ADT.

#### RECOMMENDATION 11.8

Where there have been reasonable attempts to conciliate a complaint and the Privacy Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify both parties that conciliation has failed.

### Reporting

11.46 The Privacy Commissioner may make a written report as to any “findings or recommendations” in relation to a complaint dealt with by the Commissioner. This report may be provided to the complainant, or any other people or bodies “materially involved”.<sup>93</sup> It has been suggested that “it would be beneficial to have a provision which clearly states that the Privacy Commissioner can reach findings as to breaches of IPPs or other applicable standards, in determining whether or not there has been a ‘violation of, or interference with’ a person’s privacy”.<sup>94</sup> It has also been argued that s 50 should be amended to clarify “whether a report can be issued as part of a conciliation and/or even if the complaint has been conciliated”.<sup>95</sup> We believe that such findings are within the scope of s 50 and that it should be amended to clarify this position.

---

determined fairly on the basis of written submissions by the parties: ALRC Report 108, vol 2, Recommendation 49-13.

92. See Recommendation 9.1.

93. *Privacy and Personal Information Protection Act 1998* (NSW) s 50. See also *Health Records and Information Privacy Act 2002* (NSW) s 47.

94. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 105.

95. Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 106.

**RECOMMENDATION 11.9**

Section 50 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to state that findings and recommendations can include:

- a finding that, in the opinion of the Privacy Commissioner, there has been a contravention of privacy legislation; and
- matters relating to a conciliation that has been undertaken under s 49.

11.47 We also believe that this reporting power should be extended to include “findings and recommendations” as a result of an investigation conducted by the Privacy Commissioner that is not necessarily attached to a complaint.<sup>96</sup> This will allow for flexibility when reporting under PPIPA and also allow for reports to be made to people or bodies “materially involved” after the Privacy Commissioner exercises his or her proposed own motion investigation or audit powers.<sup>97</sup>

**RECOMMENDATION 11.10**

Section 50 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to allow the Commissioner to make a written report of findings and recommendations as a result of any investigation.

11.48 Reports and recommendations of the Privacy Commissioner under HRIPA are admissible in subsequent proceedings under complaints handling provisions applicable to the private sector.<sup>98</sup> We have recommended that in certain circumstances, where a complaint has been made to the Privacy Commissioner, external review by the ADT should be allowed.<sup>99</sup> If the Privacy Commissioner has produced a report under s 50, such a report should be admissible in subsequent external review proceedings.

---

96. See Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 106-107.

97. See Recommendations 10.5, 10.7-10.8.

98. *Health Records and Information Privacy Act 2002* (NSW) s 47.

99. Recommendation 9.1.



**RECOMMENDATION 11.11**

Reports made by the Privacy Commissioner under s 50 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be admissible in subsequent external review proceedings relating to the complaint.

11.49 The Privacy Commissioner also has the power to make a special report to Parliament on any matter arising in connection with the discharge of his or her functions.<sup>100</sup> This includes matters relating to a complaint under s 45.<sup>101</sup>

**Representative complaints**

11.50 The *Privacy Act 1988* (Cth) provides for the making of “representative complaints” (interference with the privacy of two or more individuals)<sup>102</sup> where class members have complaints against the same person; all complaints are related to the same or similar circumstances; and all complaints “give rise to a substantial common issue of law or fact”.<sup>103</sup> Any member of the class can bring the complaint.<sup>104</sup> The Commonwealth Privacy Commissioner has the power to determine whether a complaint should no longer continue as a representative complaint<sup>105</sup> and also amend a complaint so it is dealt with as a representative complaint.<sup>106</sup>

11.51 We believe there may be merit in including similar provisions in NSW privacy legislation.<sup>107</sup> However we make no recommendations in

---

100. *Privacy and Personal Information Protection Act 1998* (NSW) s 65. This is discussed at para 10.28-10.33.

101. See para 10.33.

102. *Privacy Act 1988* (Cth) s 36(2).

103. *Privacy Act 1988* (Cth) s 38(1)(c).

104. *Privacy Act 1988* (Cth) s 36(2). The ALRC has recommended amending the *Privacy Act 1988* (Cth) to allow for a class member to withdraw from a representative complaint at any time if they have not consented to being a class member: ALRC, Report 108, vol 2, Recommendation 49-9.

105. *Privacy Act 1988* (Cth) s 38A.

106. *Privacy Act 1988* (Cth) s 38C.

107. Privacy NSW has recommended that the s45(1) be amended to allow representative complaints to be made to the Privacy Commissioner: Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998* (2004) 103.

relation to representative complaints in this report. We believe that it is appropriate for this issue to be addressed as part of a broader review of class actions in NSW.

## ENFORCEABLE REMEDIES

11.52 The ALRC noted that the Commonwealth Privacy Commissioner lacked the power to prescribe how respondents should act in the future – only that they should not repeat or continue conduct that constitutes an interference with the privacy of an individual.<sup>108</sup> This means that the Commonwealth Privacy Commissioner only has limited capacity to address “systemic issues”, that is, issues that are related to an organisation’s or industry’s practice rather than the specific incident itself.<sup>109</sup> To address this, the ALRC recommended that the *Privacy Act 1988* (Cth) be amended to empower the Commonwealth Privacy Commissioner to prescribe steps that an agency or respondent must take to ensure compliance with the Act in a determination.<sup>110</sup>

11.53 Complaints to the NSW Privacy Commissioner do not give rise to enforceable remedies; that is to say, the Commissioner does not have the power to make binding orders or recommendations. However, we recommend that a complainant should be able to request external review by the ADT where conciliation has failed.<sup>111</sup> This may give rise to enforceable remedies. We also make a number of recommendations to address systemic issues.<sup>112</sup> In chapter 9 we note that, if adequate resources become available, consideration should be given to empowering the Privacy Commissioner to issue reviewable determinations subsequent to a complaint.<sup>113</sup> If this is implemented, consideration should also be given to empowering the Commissioner to prescribe steps required to ensure compliance with a determination.

---

108. ALRC Report 108, vol 2, [49.47].

109. ALRC Report 108, vol 2, [49.10].

110. ALRC Report 108, vol 2, Recommendation 49-6.

111. Recommendations 9.1 and 11.8.

112. See Recommendations 10.5 and 10.7-10.10.

113. See para 9.22-9.24.

12.

## **Internal and external review**

- Introduction
- Application
- Internal review
- External review

## INTRODUCTION

12.1 In this chapter we consider the entitlement to review of agency conduct under NSW privacy legislation. This includes the right to require an agency to conduct an internal review of conduct that may be a contravention of the *Privacy and Personal Information Protection Act 1998* (NSW) (“PPIPA”). Review provisions also include a further right to request external review by the Administrative Decisions Tribunal (“ADT”), where an applicant is dissatisfied with the findings of, or action taken by, an agency in response to an internal review application. We recommend, in chapter 9, that external review by the ADT also be permitted in certain circumstances following a complaint to the Privacy Commissioner.<sup>1</sup> In this chapter we consider the time limits and orders that should apply, if our recommendation is adopted.

## APPLICATION

12.2 The internal and external review provisions in PPIPA apply to a contravention of an Information Protection Principle (“IPP”), privacy code of practice or public register provision.<sup>2</sup> We recommend that contravention of data breach provisions should trigger the same enforcement processes as breach of an IPP.<sup>3</sup> Therefore, the application of review provisions should be expanded to include a contravention of data breach notification provisions.

### RECOMMENDATION 12.1

Internal and external review under Part 5 of the *Privacy and Personal Information Protection Act 1998* (NSW) should apply to contravention of data breach notification provisions.

## INTERNAL REVIEW

12.3 Where there has been a contravention of an IPP, privacy code of practice or public register provision, a “person aggrieved” by the “conduct” of an agency is entitled to request internal review of that

- 
1. See Recommendation 9.1.
  2. *Privacy and Personal Information Protection Act 1998* (NSW) s 52.
  3. See Recommendation 9.2.

conduct.<sup>4</sup> An internal review must be conducted by the public sector agency concerned.<sup>5</sup>

12.4 If undertaken by the agency, the review must be conducted by an employee or officer of the agency who, “as far as is practicable”, was not substantially involved in the matters relating to the conduct raised and who is suitably qualified to deal with the matters raised in the application. While conducting the review, the individual must consider relevant material submitted by the applicant and the Privacy Commissioner.<sup>6</sup>

12.5 This review must be conducted “as soon as is reasonably practicable in the circumstances”. However, if the review is not conducted within 60 days of receipt of the application, the applicant may apply for ADT review under s 55 of PPIPA.<sup>7</sup>

12.6 After conducting the review the public sector agency can choose to take no action or:<sup>8</sup>

- make a formal apology;
- take remedial action as it thinks appropriate including the payment of compensation;<sup>9</sup>
- provide undertakings that the conduct will not occur again; and/or
- implement administrative measures to ensure that the conduct will not occur again.

12.7 The public sector agency must notify the applicant in writing of the finding of the review, action proposed to be taken by the agency, and the right of the applicant to have proposed actions reviewed by the ADT.<sup>10</sup>

---

4. *Privacy and Personal Information Protection Act 1998* (NSW) s 52, s 53.

5. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(2). The Privacy Commissioner, upon the request of the agency, can also conduct the internal review: *Privacy and Personal Information Protection Act 1998* (NSW) s 54(5).

6. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(4)-53(5).

7. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(6).

8. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(7).

9. Unless the conduct relates to a convicted inmate: *Privacy and Personal Information Protection Act 1998* (NSW) s 53(7A).

### “Person aggrieved”

12.8 A person who is “aggrieved” by the conduct of a public sector agency is entitled to a review of that conduct.<sup>11</sup> PPIPA does not define the term “person aggrieved”. A “person aggrieved” is not limited to the person who is the subject of the personal information at issue.<sup>12</sup> It may include a person who has been specifically and adversely affected by the alleged breach of PPIPA, such as the parent of a person who has had his or her information disclosed.<sup>13</sup> Whether a person is aggrieved by the conduct of an agency is ultimately a question of fact to be determined depending on the circumstances of each case.<sup>14</sup> In *GA v Department of Education and Training*, the ADT held that PPIPA is “beneficial legislation and accordingly a broad interpretation of the words ‘person aggrieved’ is appropriate”, but emphasised that “the person must nevertheless be ‘aggrieved’ because he or she believes that the conduct constitutes a breach of [PPIPA], not for any extraneous reason”.<sup>15</sup>

### “Conduct”

12.9 “Conduct” refers to what an “agency did or did not do with [an individual’s] personal information”.<sup>16</sup> It is the contravention by a public sector agency of an IPP or privacy code of practice that applies to the agency, or the disclosure by a public sector agency of personal information kept in a public register.<sup>17</sup> The conduct must have occurred at the time the internal review application was made and does not include

- 
10. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(8). This must occur as soon as practicable after completion, or in any event must be within 14 days.
  11. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(1).
  12. *NR v Roads and Traffic Authority* [2004] NSWADT 276.
  13. *KO v Commissioner of Police, NSW Police* [2004] NSWADT 3, [18]. But will not include a parent where the child is an adult, the information relates exclusively to the child and there is no evidence of the child consenting to or supporting the parent’s application: *GA v Department of Education and Training* [2005] NSWADT 47, [12]. See also *ZR v NSW Dept of Education and Training* [2008] NSWADT 199, [118].
  14. *GA v Department of Education and Training* [2005] NSWADT 47, [12]; *ZR v NSW Dept of Education and Training* [2008] NSWADT 199, [118].
  15. *GA v Department of Education and Training* [2005] NSWADT 47, [8]. See also *GA v Department of Education and Training* [2005] NSWADTAP 64.
  16. *Department of Education and Training v GA (No 3)* [2004] NSWADT 50, [5].
  17. *Privacy and Personal Information Protection Act 1998* (NSW) s 52(1).

“possible future conduct” or subsequent conduct.<sup>18</sup> A reference to “conduct” in Part 5 of PPIPA includes a reference to “alleged conduct”.<sup>19</sup> This allows an individual to seek a review of conduct that he or she believes has occurred but about which he or she does not have sufficient knowledge or particulars.<sup>20</sup>

12.10 This may demonstrate that the “NSW review process [cannot] be used to change policy or practice to prevent a breach, only to provide a remedy after a breach”.<sup>21</sup> We have made a number of recommendations – for example, providing the Privacy Commissioner with audit powers as well as injunction and own motion investigation powers – which will help to address this concern.

### The role of the Privacy Commissioner

12.11 The Privacy Commissioner is given an oversight role in relation to internal reviews. If an agency receives an application for internal review it must notify the Privacy Commissioner; keep the Commissioner informed of the review’s progress; and inform the Commissioner of the findings of the review and proposed action by the agency. The Privacy Commissioner is entitled to make submissions to the agency in relation to the matter.<sup>22</sup>

12.12 The Privacy Commissioner can, at the request of the agency, undertake the review on behalf of the agency and report to the agency in relation to the application.<sup>23</sup> However, due to conflict of interest issues, the Commissioner has been reluctant to accept these requests.<sup>24</sup> It has been suggested that some smaller agencies “often find it difficult to find a

---

18. *Wykanak v Director General, Department of Local Government* [2002] NSWADT 208, [17]-[18].

19. *Privacy and Personal Information Protection Act 1998* (NSW) s 52(2).

20. *ON v Marrickville Council* [2005] NSWADT 274, [32].

21. N Waters, A Paramaguru and A Johnston, *Working Paper No 3: Enforcement of privacy laws – issues arising from Australian experience v. 2* (2007) 9.

22. *Privacy and Personal Information Protection Act 1998* (NSW) s 54(1)-54(2).

23. *Privacy and Personal Information Protection Act 1998* (NSW) s 54(3). The Commissioner is entitled to charge an appropriate fee for review: s 54(4). Sections 53(7)-(8) also apply to the Privacy Commissioner if it is conducting a review on behalf of an agency: s 54(5).

24. Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 114.

suitably qualified employee who is also independent of the conduct or decision under review” and it would be worthwhile permitting agencies to outsource internal reviews obligations.<sup>25</sup> The Government notes that “internal reviews are best addressed by an agency’s own management structures” but it may be useful to permit smaller agencies to outsource such obligations.<sup>26</sup> We recommend, as did the Statutory Review of PPIPA, that agencies should be able to out source their internal review obligations to appropriately qualified agents.

## RECOMMENDATION 12.2

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

### Time limits – applicant

12.13 In addition to other application requirements the application for review must be “lodged at an office of the public sector agency within 6 months (or such later date as the agency may allow) from the time the applicant first became aware of the conduct the subject of the application”.<sup>27</sup>

12.14 In CP 3 we asked whether s 53(3) of PPIPA should be amended to include a provision allowing a person to request internal review of conduct outside the six-month limitation period.<sup>28</sup> Many submissions supported allowing out of time requests in particular circumstances<sup>29</sup> noting that the limitation disadvantages applicants who may first attempt

25. Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 114-115. NSW Attorney General’s Department, *Review of the Privacy and Personal Information Protection Act 1998* (Tabled 25 September 2007, Legislative Assembly) (“Statutory Review of PPIPA”) Recommendation 24.

26. NSW Government, *Response to the Report on the Statutory Review of the Privacy and Personal Information Protection Act 1998*, 11.

27. *Privacy and Personal Information Protection Act 1998* (NSW) s 53(3)(d).

28. NSW Law Reform Commission, *Privacy Legislation in NSW*, Consultation Paper 3 (2008) (“NSWLRC CP 3”) Issue 60.

29. Cyberspace Law and Policy Centre, *Submission*, 34; Inner City Legal Centre, *Submission*, 43; Privacy NSW, *Submission*, 12; Public Interest Advocacy Centre, *Submission*, 30.



to resolve a matter informally.<sup>30</sup> The Public Interest Advocacy Centre (“PIAC”) has cautioned that due to the complexity of privacy legislation, an individual may be aware of conduct, but may not be aware of a breach.<sup>31</sup> The Inner City Legal Centre further submitted that refusal of such a request should be reviewable by the ADT.<sup>32</sup> Conversely, submissions noted that permitting out of time requests would make it difficult for agencies to investigate alleged breaches.<sup>33</sup>

12.15 We are of the view that internal review of conduct should be permitted outside the six-month limitation period in exceptional circumstances.

### RECOMMENDATION 12.3

Sub-section 53(3) of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to allow for individuals, in exceptional circumstances, to request internal review of conduct outside the six-month limitation period.

### Time limits – agencies

12.16 PIAC submits that penalties should apply to agencies that fail to conduct their internal review within 60 days. They note that the process can be stressful for applicants and unlike discrimination laws there is no protection against victimisation and, additionally, many applicants are cautious about going to the ADT because of the costs involved.<sup>34</sup>

12.17 We do not recommend imposing penalties on agencies that fail to conduct a review within the prescribed time. However, we do make a number of recommendations that will both protect applicants against

30. Statutory Review of PPIPA, [14.29].

31. Public Interest Advocacy Centre, *Submission*, 30.

32. Inner City Legal Centre, *Submission*, 43.

33. NSW FOI/Privacy Practitioners’ Network, *Submission*, 12. NSW Department of Corrective Services, *Submission*, 6 notes, “the current six-month limitation period works reasonably well and any longer period could result in poor recall of witnesses and the ability to find evidence”.

34. Public Interest Advocacy Centre, *Submission*, 30.

victimisation<sup>35</sup> and provide a more flexible framework for enforcement of privacy legislation.<sup>36</sup>

## EXTERNAL REVIEW

12.18 If a person (“the applicant”) is dissatisfied with the findings of an internal review, or the actions taken by the public sector agency in relation to the application for internal review, he or she can apply to the ADT to review the conduct that was the subject of the internal review application.<sup>37</sup>

### Jurisdiction

12.19 In CP 3 we asked whether s 55 of PPIPA should be amended to clarify whether an application to the ADT is heard in its original or review jurisdiction and whether the jurisdiction should be specified as being “review”.<sup>38</sup> 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”<sup>39</sup> whereas a “reviewable decision” is “a decision of an administrator that the Tribunal has jurisdiction under an enactment to review”.<sup>40</sup> The ADT has different powers available depending on the applicable jurisdiction, for example, the power to award costs is available under its review jurisdiction but not its original jurisdiction.<sup>41</sup> Submissions to CP 3 indicated that the ADT

---

35. See Recommendations 10.14-10.16.

36. See Recommendation 9.1.

37. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(1). For information about external review under the *Health Records and Information Privacy Act 2002* (NSW) see para 9.12. Only a small number of applications are filed in the ADT and the majority of these do not result in a decision because they have been resolved through alternate dispute resolution processes: NSW Administrative Decisions Tribunal, *Submission to Attorney General’s Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (2004) 1.

38. NSWLRC CP 3, Issue 59.

39. *Administrative Decisions Tribunal Act 1997* (NSW) s 7, s 37.

40. *Administrative Decisions Tribunal Act 1997* (NSW) s 8, s 38.

41. *Administrative Decisions Tribunal Act 1997* (NSW) s 88(3).

should approach matters under PPIPA in the same way as it deals with merits review work<sup>42</sup> and that review may be preferable jurisdiction.<sup>43</sup>

12.20 The position has since been clarified with the passage of the *Administrative Decisions Tribunal Amendment Act 2008* (NSW) (“ADTA Act”), which provides that “[t]he jurisdiction conferred on the Tribunal by section 55 of the *Privacy and Personal Information Protection Act 1998* is an example of jurisdiction to review conduct”.<sup>44</sup> We think that it would be beneficial to include a corresponding note in PPIPA to clarify the issue further.

12.21 Prior to the passage of the ADTA Act there were several aspects of privacy legislation that caused confusion as to the jurisdiction involved:

- (1) ***The interaction between s 55(1) and s 53(8) of PPIPA:*** Section 53(8) provides that upon completion of an internal review, the agency must notify the applicant of the findings of the review and the “right of the person to have those findings, and the agency’s proposed action, reviewed by the Tribunal”. Section 55(1), relating to external review, is different in that it entitles the applicant to apply to the Tribunal “for a review of the conduct that was the subject of the application under section 53”.<sup>45</sup> The reference to conduct has caused some confusion because “[d]iscrete decisions of an administrator, rather than

---

42. Cyberspace Law and Policy Centre, *Submission*, 33; Australian Privacy Foundation, *Submission*, 14; Privacy NSW, *Submission*, 12. Public Interest Advocacy Centre, *Submission*, 29 submits that it should be made clear that the type of review is merits review of conduct rather than review of a decision. NSW FOI/Privacy Practitioners’ Network, *Submission*, 11 views internal review decisions as “determinations” that should be reviewed by the ADT if required.

43. Business Law Committee of the Law Society, *Submission*, 14; NSW FOI/Privacy Practitioners’ Network, *Submission*, 11; Privacy NSW, *Submission*, 12; Public Interest Advocacy Centre, *Submission*, 29. Inner City Legal Centre, *Submission*, 42 does not make a specific submission in relation to the applicable jurisdiction, however notes that there should be no costs award in these cases and the burden of proof should not rest with one party over the other. It notes that “the ADT’s task is to determine what the correct and preferable approach might have been”.

44. *Administrative Decisions Tribunal Amendment Act 2008* (NSW) sch 1[1], amending *Administrative Decisions Tribunal Act 1997* (NSW) s 8, commenced January 2009.

45. *Privacy and Personal Information Protection Act 1998* (NSW). See *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [9].

conduct in which they are alleged to have engaged, are generally the subject of merits review proceedings”.<sup>46</sup>

- (2) **Section 56 right of appeal to the Appeal Panel:** PPIPA explicitly indicates that an order or decision of the ADT may be appealed to the Appeal Panel of the ADT. Specific provision for appeal is only necessary where a matter falls under the Tribunals “original” jurisdiction.<sup>47</sup>
- (3) **Remedies available under PPIPA:** The remedies available under s 55(2) comprise damages and injunctions. It has been pointed out that “[t]hese kind of remedies are not typically available in merits review proceedings”.<sup>48</sup>
- (4) **Preservation of the Tribunal’s powers to affirm, vary or set aside reviewable decisions:** Sub-section s 55(3) of PPIPA indicates that nothing in s 53 limits any other powers that the Tribunal has under Division 3, Part 3, Chapter 5 of the *Administrative Decisions Tribunal Act 1997* (NSW) (“the ADT Act”). These powers relate to “a reviewable decision”.<sup>49</sup> It has been noted that the “specific inclusion of these provisions suggests that despite the fact that damages, injunctions and other civil remedies are available in cases of this kind, the merits review outcomes are also available”. Conversely, it was also noted that if it clearly fell within the ADT’s “review”

---

46. *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [11]. Note that following the *Administrative Decisions Tribunal Amendment Act 2008* (NSW), the *Administrative Decisions Tribunal Act 1997* (NSW) s 8(2)(a) has been inserted, stating that “the conduct of an administrator (or a refusal by an administrator to engage in conduct) is a reviewable decision if the Tribunal has jurisdiction under an enactment to review the conduct or refusal”.

47. *Administrative Decisions Tribunal Act 1997* (NSW) s 112(1)(a). See also *PC v University of New South Wales (No 2)* [2005] NSWADT 264, [25]-[26]; *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [11].

48. *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [11]. See also *PC v University of New South Wales (No 2)* [2005] NSWADT 264, [35].

49. *Administrative Decisions Tribunal Act 1997* (NSW) s 63-66. See also *PC v University of New South Wales (No 2)* [2005] NSWADT 264, [30].

jurisdiction, explicit reference to the merits review outcomes would be unnecessary.<sup>50</sup>

- (5) ***The absence of the power to award costs under PPIPA:*** Subsection 88(1) of the ADT Act allows the ADT to award costs in special circumstances however the “Tribunal may not award costs in relation to proceedings for an original decision unless the enactment under which the Tribunal has jurisdiction to make the decision provides for the awarding of costs”.<sup>51</sup> PPIPA does not contain any such provision, suggesting “the legislature intended that an application under [PPIPA] is an application for a review of a reviewable decision; otherwise the Tribunal would have no costs power in relation to such applications”.<sup>52</sup>
- (6) ***HRIPA explicitly notes that the jurisdiction of the ADT is “original”:*** The note to s 48(1) of the *Health Records and Information Privacy Act 2002* (NSW) (“HRIPA”) clearly states that the ADT exercises its original jurisdiction when hearing applications for an inquiry into a complaint made to the Privacy Commissioner under that Act (applicable to the private sector). HRIPA explicitly deals with awarding costs, the right of appeal, and includes no provisions for internal review, all in line with the ADT’s “original” jurisdiction. Comparatively, a complaint in relation to public sector agencies under HRIPA triggers the PPIPA review mechanisms.<sup>53</sup> There is no mention in HRIPA of the applicable jurisdiction where review under PPIPA is referenced, and there is no special provision for costs. This may have suggested, “the jurisdiction of the Tribunal in relation to privacy complaints against public sector agencies is not intended to be an original one”.<sup>54</sup>

---

50. *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [10].

51. *Administrative Decisions Tribunal Act 1997* (NSW) s 88(3).

52. *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [10].

53. *Health Records and Information Privacy Act 2002* (NSW) s 21.

54. *PC v University of New South Wales (No 2)* [2005] NSWADT 264, [42].

- (7) *PPIPA excludes internal review provisions of the ADT Act:* Sub-section 52(4) of PPIPA indicates that s 53 of the ADT Act does not apply. It would be unnecessary to “oust the internal review provisions of the ADT Act if an application under [PPIPA] was not intended to be an application for a review of a reviewable decision”.<sup>55</sup>

12.22 Prior to the amendments as a result of the ADTA Act, the ADT held that applications under PPIPA appeared to fall within its “review” jurisdiction.<sup>56</sup> However, these decisions also noted that legislative intention was “not consistent”<sup>57</sup> and “less than clear”.<sup>58</sup>

#### RECOMMENDATION 12.4

The *Privacy and Personal Information Protection Act 1998* (NSW) should include a note stating that application to the Administrative Decisions Tribunal, following an internal review, is heard in the Tribunal’s “review” jurisdiction.

#### Time limits

12.23 Under PPIPA there is no time limit to apply for review by the ADT.<sup>59</sup> The ADT suggests that 60 days after completion of the internal

55. *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [10]. See also *PC v University of New South Wales (No 2)* [2005] NSWADT 264, [10]-[11].

56. *PC v University of New South Wales (No 2)* [2005] NSWADT 264; *PC v University of New South Wales (No 2)* [2006] NSWADTAP 54; *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132; *BQ v Commissioner of Police, New South Wales Police Service* [2002] NSWADT 64. The ADT has found that “there is a basis for concluding that at least part of what the Tribunal is doing in a Privacy Act matter is reviewing the decision of the agency to the extent that its findings come under review, or the action taken or proposed to be taken come under review”: *PC v University of New South Wales (No 2)* [2005] NSWADT 264, [30].

57. *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, [12].

58. *PC v University of New South Wales (No 2)* [2005] NSWADT 264, [8]. See also *PC v University of New South Wales (No 2)* [2006] NSWADTAP 54, [6]; *JW v Pittwater Council* [2009] NSWADT 4, [4].

59. Legal Aid NSW noted the decision in *GQ v NSW Department of Education and Training* [2008] NSWADT 212 that the 28 day period outlined in the Interim

review would be an appropriate time limit. Further, the ADT submits that a provision should be added allowing a person who lodges a complaint with the Privacy Commissioner within time to preserve a right to apply to the ADT for external review until after the complaints handling process is completed.<sup>60</sup>

12.24 In CP 3 we proposed that PPIPA should be amended to include a limitation period for application for external review by the ADT following internal review. We recommended that this should provide that an application to the ADT 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.<sup>61</sup> Submissions supported imposing time limits on application to the ADT.<sup>62</sup> However, many noted, and we agree, that the proposal should be clarified to apply to matters following an internal review, not simply a complaint to the Privacy Commissioner.<sup>63</sup>

12.25 The absence of applicable time limits will make it difficult for agencies to defend their actions "as facts, evidence and the recall of any witnesses are lost or destroyed with time"<sup>64</sup> and it is an "unreasonable

---

ADT rules does not apply to appeals under the *Privacy and Personal Information Protection Act 1998* (NSW) s 55 and is "confusing for litigants, who are often not independently legally advised, and creates complications for agencies when advising internal review applicants of their appeal rights": Legal Aid NSW, *Submission*, 3. Compare *Health Records and Information Privacy Act 2002* (NSW) s 48(2). An application may only be made within 28 days after the complainant received the report of the Privacy Commissioner or the day recommended in the report of the Commissioner as the day on which an application may be made to the Tribunal (whichever is later).

60. NSW Administrative Decisions Tribunal, *Submission to Attorney General's Department Review of the Operation of the Privacy and Personal Information Protection Act 1998* (2004) 9.

61. NSWLRC CP 3, Proposal 18.

62. Cyberspace Law and Policy Centre, *Submission*, 33; Inner City Legal Centre, *Submission*, 19; Legal Aid NSW, *Submission*, 3; NSW Department of Corrective Services, *Submission*, 2; NSW Department of Education and Training, *Submission*, 8; Privacy NSW, *Submission*, 4; Public Interest Advocacy Centre, *Submission*, 29.

63. Cyberspace Law and Policy Centre, *Submission*, 33; Cyberspace Law and Policy Centre, *Submission*, 33; NSW FOI/Privacy Practitioners' Network, *Submission*, 2.

64. NSW Department of Corrective Services, *Submission*, 2.

impost” on agencies.<sup>65</sup> The ADT has recommended “urgent consideration be given to amending [PPIPA] or the ADT Act so as to fix a time limit for lodgement of applications for review of conduct with the Tribunal, and to allow a power to extend if there is a reasonable explanation for delay”.<sup>66</sup> We agree that a reasonable time limit for appeal to the ADT should be imposed.<sup>67</sup> We have recommended that a complaint to the Privacy Commissioner trigger ADT review where the complainant has been notified that the conciliation has failed.<sup>68</sup> This is reflected, with respect to time limits, in the recommendation below. We believe, as did a number of submissions, that out of time requests should be permitted in exceptional circumstances. For example, where the applicant had health problems or difficulty obtaining necessary legal representation.<sup>69</sup>

12.26 We also recommend that the Privacy Commissioner and/or the agency should inform the applicants of their right to a review by the ADT and also the time limits that apply.<sup>70</sup>

#### RECOMMENDATION 12.5

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include a limitation period for application to the Administrative Decisions Tribunal for review so that an application for external review of a complaint must be made within 60 days after:

- (1) the complainant is notified by the Privacy Commissioner that the conciliation has failed;
- (2) the applicant receives notification of the findings of an internal review under s 53(8); or
- (3) the agency has failed to notify the applicant of the findings of the review within the prescribed time (74 days).

65. Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 119.

66. *AT v Commissioner of Police, New South Wales Police Force (GD)* [2009] NSWADTAP 1, [42]. See also Statutory Review of PPIPA, Recommendation 26.

67. We note that an agency must complete an internal review within 60 days, and has a further 14 days to issue findings: *Privacy and Personal Information Protection Act 1998* (NSW) s 53.

68. See Recommendation 9.1.

69. Inner City Legal Centre, *Submission*, 19; Public Interest Advocacy Centre, *Submission*, 29.

70. This was supported by Inner City Legal Centre, *Submission*, 19.



**RECOMMENDATION 12.6**

The Administrative Decisions Tribunal should permit out of time requests for review in exceptional circumstances.

**RECOMMENDATION 12.7**

The Privacy Commissioner or relevant agency should inform all complainants or internal review applicants of any relevant right to review by the Administrative Decisions Tribunal and also the time limits that apply.

**Tribunal orders**

12.27 The ADT can take no action or it can order that the public sector agency:<sup>71</sup>

- pay damages to the applicant (subject to particular limitations);<sup>72</sup>
- refrain from conduct that contravenes an IPP or privacy code of practice;
- perform the requirements of an IPP or privacy code of practice;
- correct personal information that has been disclosed;
- take specific steps to remedy loss or damage suffered by the applicant; and
- not disclose personal information contained in a public register.

12.28 The ADT can also make any ancillary orders it thinks appropriate.<sup>73</sup> If the ADT considers that the CEO or an employee of the agency has failed to exercise his or her functions in good faith, the Tribunal is permitted to take measures to bring the conduct to the attention of the

---

71. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(2). See also *Health Records and Information Privacy Act 2002* (NSW) s 54. Note that failure to comply with particular ADT orders under the *Health Records and Information Privacy Act 2002* (NSW) is an offence: s 56.

72. The Tribunal can only award damages if they are satisfied that the applicant has suffered financial loss or psychological or physical harm. As with internal review procedures, damages cannot be paid if the conduct relates to a convicted inmate: *Privacy and Personal Information Protection Act 1998* (NSW) s 55(4), s 55(4A). See also *Health Records and Information Privacy Act 2002* (NSW) s 54(1)(a), s 54(2).

73. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(2)(g).

responsible Minister for the agency.<sup>74</sup> The ADT may also exercise its “powers on review” under the ADT Act.<sup>75</sup>

12.29 We recommend that internal and external review should apply to failure to comply with proposed data breach notification provisions.<sup>76</sup> Accordingly, the ADT should be empowered to order that an agency notify individuals of a data breach as required by data breach notification provisions.

#### RECOMMENDATION 12.8

If Recommendation 9.2 is adopted, the Administrative Decisions Tribunal should be able to make an order requiring a public sector agency to comply with notification requirements in data breach notification provisions.

#### *Limited to infringing conduct?*

12.30 It is unclear whether orders can only be made in respect of infringing conduct or can also include conduct that is merely alleged. In CP 3 the Commission proposed that s 55(2) of PPIPA should be amended to provide that the ADT may make any one or more of the orders listed in paragraphs (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.<sup>77</sup>

12.31 Submissions were divided on this issue, some were generally supportive,<sup>78</sup> and others submitted that the proposal would limit

74. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(5).

75. See *Privacy and Personal Information Protection Act 1998* (NSW) s 55(3). For example, the Tribunal may affirm, vary, set aside, substitute a decision or remit the matter for reconsideration by the administrator in accordance with directions or recommendations of the Tribunal: *Administrative Decisions Tribunal Act 1997* (NSW) s 63-66.

76. Recommendation 9.2.

77. NSWLRC CP 3, Proposal 19.

78. Privacy NSW, *Submission*, 4; Cyberspace Law and Policy Centre, *Submission*, 34; NSW Department of Education and Training, *Submission*, 8; NSW Department of Primary Industries, *Submission*; NSW FOI/Privacy Practitioners’ Network, *Submission*, 2; Australian Privacy Foundation, *Submission*, 14.

flexibility when granting remedies.<sup>79</sup> For example, the Inner City Legal Centre points out that the:

power to make orders is quite wide ranging and it is conceivable that orders may be appropriate to deal with situations where the evidence is prosaic or uncertain. An example might be where a disclosure or contravention has occurred but the source is uncertain or only suspected. In such a case a range of protective and corrective orders may be appropriate to protect the individual in the future.<sup>80</sup>

12.32 We do not believe that PPIPA should be amended to explicitly require the ADT to find a contravention prior to making orders. Such a requirement would unnecessarily restrict the flexibility of the ADT's powers and prevents the ADT from better addressing systemic issues where appropriate.

### *Systemic issues*

12.33 In *FM v Vice Chancellor, Macquarie University*,<sup>81</sup> the ADT ordered that the "[t]he Vice Chancellor, Macquarie University and any person employed or engaged by Macquarie University, is to restrain from disclosing information or opinions in relation to students or former students, which is held in their minds, unless an exemption relating to s 18 applies". The Appeal Panel subsequently found that:

the order is expressed as a systemic, agency-wide order. This is problematic. In our view, unless there are good reasons to make a wider systemic order, orders should be confined to the parties to the proceedings. In our view no case was advanced by FM that went beyond what happened to him and its lawfulness. Orders should, as we see it, be inter partes unless there has been considered attention given in the proceedings to the possibility of a wider-operating order. Obviously in well-administered organisations the order will be adopted as a precedent and a basis for policy that will govern all practice of a like kind.<sup>82</sup>

---

79. Inner City Legal Centre, *Submission*, 19; Public Interest Advocacy Centre, *Submission*, 31.

80. Inner City Legal Centre, *Submission*, 19.

81. *FM v Vice Chancellor, Macquarie University* [2003] NSWADT 78. Note subsequent appeals: *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43; *Vice-Chancellor, Macquarie University v FM (No.2) (GD)* [2004] NSWADTAP 37; *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192. Orders of the Tribunal were ultimately set aside.

82. *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43, [125].

12.34 Concerns have been expressed in relation to the reluctance of the ADT to impose systemic remedies unless there is evidence demonstrating a systemic problem. It has been noted, “neither the applicants nor the Privacy Commissioner are likely to be in a position to provide evidence of systemic problems”.<sup>83</sup> This demonstrates the limitations of the adversarial model to produce systemic change. In our view, the requirement that appropriate evidence is presented prior to orders being made by the ADT is appropriate in the context of such proceedings. The Privacy Commissioner is in the best position to address systemic problems, and our recommendations in chapter 10 bolster the powers of the Commissioner to achieve this.<sup>84</sup>

#### *Privacy Commissioner conciliation*

12.35 We recommend that external review by the ADT be permitted where Privacy Commissioner conciliation is unsuccessful.<sup>85</sup> We note that such a review would likely have to take place under the ADT’s original jurisdiction.<sup>86</sup> We believe that matters before the ADT following an unsuccessful conciliation should be handled as consistently as possible with matters following an internal review. The ADT’s powers, especially in relation to orders, should be consistent with powers subsequent to an internal review by an agency.<sup>87</sup>

### RECOMMENDATION 12.9

If Recommendation 9.1 is adopted, the orders that can be made by the Administrative Decisions Tribunal subsequent to a complaint to the Privacy Commissioner should be consistent with the orders that can be made under s 55(2) of the *Privacy and Personal Information Protection Act 1998* (NSW).

### The role of the Privacy Commissioner

12.36 The ADT must notify the Privacy Commissioner that it has been requested to review an internal review and the Privacy Commissioner

83. Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 123.

84. See, eg, Recommendation 10.5.

85. See Recommendation 9.1.

86. See para 9.26.

87. It may also be necessary to include specific provision to award costs, as in the *Health Records and Information Privacy Act 2002* (NSW) s 55. See para 12.21(6).

has the right to appear and be heard in these proceedings.<sup>88</sup> The precise role of the Commissioner in relation to ADT proceedings is unclear.<sup>89</sup> The Statutory Review of PPIPA recommended, and we agree, that PPIPA should set out the scope of the Commissioner's role and this should be established in consultation with the Commissioner and the President of the ADT. The primary role should be "to assist in matters of statutory interpretation and privacy practice in NSW".<sup>90</sup> The Government supports this recommendation in principle, and has noted that it will help clarify that the role of the Commissioner is not to advocate on behalf of applicants.<sup>91</sup>

#### RECOMMENDATION 12.10

The *Privacy and Personal Information Protection Act 1998* (NSW) should set out the scope of the Privacy Commissioner's role in the Administrative Decisions Tribunal. This should be determined in consultation with the Privacy Commissioner and the President of the Administrative Decisions Tribunal. The primary role should be to assist in matters of statutory interpretation and privacy practice in NSW.

#### *Appeal panel*

12.37 Orders or decisions made by the ADT may be appealed to the ADT's Appeal Panel.<sup>92</sup> However, the Privacy Commissioner does not have a clear right to appear before the Appeal Panel. In CP 3 we proposed that s 56 of PPIPA be amended to include a provision that the Privacy Commissioner has the right to appear and be heard in any proceedings before the Appeal Panel of the ADT. Submissions supported this

88. *Privacy and Personal Information Protection Act 1998* (NSW) s 55(6)-55(7).

89. See Privacy NSW, *Submission by Privacy NSW on the Review of the Privacy and Personal Information Protection Act 1998* (2004) 121-122; Statutory Review of PPIPA, 70-71.

90. Statutory Review of PPIPA, Recommendation 25.

91. NSW Government, Response to the Report on the Statutory Review of the *Privacy and Personal Information Protection Act 1998*, 11.

92. *Privacy and Personal Information Protection Act 1998* (NSW) s 56. See also *Health Records and Information Privacy Act 2002* (NSW) s 57.

proposal.<sup>93</sup> The ADT has noted that the Privacy Commissioner plays a “central role” in privacy legislation:

The Privacy Commissioner has an oversight role in relation to the way agencies handle complaints. There are many other powers and responsibilities given to the Privacy Commissioner by other parts of the Privacy Act of similar significance. It would make a mockery of these arrangements for the Privacy Commissioner to be cut out of the appeals environment of the Tribunal, where quite possibly some of the most significant questions touching on the scope and operation of the legislation might arise.<sup>94</sup>

12.38 We agree with this view, and believe that s 56 of PPIPA should be amended to explicitly include this right. As under s 55(6), the Privacy Commissioner should also be notified of an application to the Appeal Panel under s 56.<sup>95</sup>

#### RECOMMENDATION 12.11

Section 56 of the *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to include provisions that the Privacy Commissioner:

- (1) is to be notified by the Tribunal of any application made to it under s 56; and
- (2) has a right to appear and be heard in any proceedings before the Tribunal in relation to a review under s 56.

#### *Privacy Commissioner conciliation*

12.39 Additionally, if our recommendation to allow external review of conduct where the complainant is notified that conciliation has failed is adopted, the Privacy Commissioner should have the right to appear and

93. Privacy NSW, *Submission*, 4; Inner City Legal Centre, *Submission*, 20; NSW FOI/Privacy Practitioners’ Network, *Submission*, 2; Cyberspace Law and Policy Centre, *Submission*, 34; Public Interest Advocacy Centre, *Submission*, 31. NSW Department of Education and Training, *Submission*, 9 “does not object” to this proposal but expressed surprise that the amendment is considered necessary. Also see Statutory Review of PPIPA, Recommendation 25.

94. *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43, [41].

95. See Public Interest Advocacy Centre, *Submission*, 31.

be heard in external review proceedings.<sup>96</sup> We note that such proceedings would likely be conducted under the ADT's "original" jurisdiction.<sup>97</sup>

#### RECOMMENDATION 12.12

---

If Recommendation 9.1 is adopted, the Privacy Commissioner should have the right to appear and be heard in any proceedings before the Administrative Decisions Tribunal where external review is being conducted subsequent to a complaint to the Privacy Commissioner.

---

96. Recommendation 9.1.

97. See para 9.26. Note a similar requirement is in the *Health Records and Information Privacy Act 2002* (NSW) s 50, where the Tribunal performs external review in relation to the private sector under their "original" jurisdiction.





**Appendix A:  
Comparative table  
of definitions of  
public sector  
agency**

GIPA Act – agency (s 4)	Privacy Act (Cth) – agency (s 6)	Privacy Act (Cth) – State and Territory authority (s 6C)	PPIPA (s 3)
(a) Government Department, Sch 4: Government Department means a Department under the <i>Public Sector Employment and Management Act 2002</i> (NSW)	(b) a Department	(b) a Department of State of a State or Territory	(a) a government department or the Teaching Service
(b) a Minister (including a Minister's personal staff)	(a) a Minister	(a) a State or Territory Minister	
(c) a public authority Sch 4 cl 2 (a) a statutory body representing the Crown, or			(b) a statutory body representing the Crown
Sch 4 cl 2 (b) a body (whether incorporated or unincorporated) established or continued for a public purpose by or under the provisions of a legislative instrument, or	(c) a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:  (i) an incorporated company, society or association; or...	(c) a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a law of a State or Territory, other than:  (i) an incorporated company, society or association; or  (ii) an association of employers or employees that is registered or recognised under a law of a State or Territory dealing with the resolution of industrial disputes	<i>Potentially:</i>  (c) a declared authority under the <i>Public Sector Management Act 1988</i> (NSW)  (d) a person or body in relation to whom, or to whose functions, an account is kept of administration or working expenses, if the account:  (i) is part of the accounts prepared under the <i>Public Finance and Audit Act 1983</i> (NSW).
Sch 4 cl 2 (c) the NSW Police Force, or	(h) the Australian Federal Police		(e) the NSW Police Force
Sch 4 cl 2 (d) the Teaching Service, or			(a) a government department or the Teaching Service

GIPA Act – agency (s 4)	Privacy Act (Cth) – agency (s 6)	Privacy Act (Cth) – State and Territory authority (s 6C)	PPIPA (s 3)
Sch 4 cl 2 (e) a State owned corporation, or	(c) a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment	(c) a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a law of a State or Territory	Explicitly excluded: “but does not include a State owned corporation”.
Sch 4 cl 2 (f) a wholly-owned subsidiary of the Crown in right of the State or of a public authority, or			
Sch 4 cl 2 (g) a body declared to be a public authority by a regulation under [Sch 4 cl 2].			
<p>Sch 4 cl 2 (2) The regulations may declare any of the following bodies to be a public authority:</p> <p>(a) a body (whether incorporated or unincorporated) established for a public purpose otherwise than by or under the provisions of a legislative instrument,</p> <p>(b) a body (whether incorporated or unincorporated) that is established by the Governor or by a Minister or that is an incorporated company or association over which a Minister is in a position to exercise direction or control.</p>	(d) a body established or appointed by the Governor General, or by a Minister, otherwise than by or under a Commonwealth enactment; or	<p>(d) a body established or appointed, otherwise than by or under a law of a State or Territory, by:</p> <p>(i) a Governor of a State; or</p> <p>...</p> <p>(v) a State or Territory Minister; or</p> <p>...</p>	<p><i>Potentially:</i></p> <p>(c) a declared authority under the <i>Public Sector Management Act 1988</i> (NSW),</p> <p>(d) a person or body in relation to whom, or to whose functions, an account is kept of administration or working expenses, if the account:</p> <p>(i) is part of the accounts prepared under the <i>Public Finance and Audit Act 1983</i> (NSW).</p>

GIPA Act – agency (s 4)	Privacy Act (Cth) – agency (s 6)	Privacy Act (Cth) – State and Territory authority (s 6C)	PPIPA (s 3)
<p>(d) a public office Sch 4 cl 3</p> <p>(a) an office established or continued for a public purpose by or under the provisions of a legislative instrument, or</p> <p>(b) any other office to which an appointment is made by the Governor or by a Minister that is declared by the regulations to be a public office</p>	<p>(e) a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department;</p> <p>(f) a person holding or performing the duties of an appointment, being an appointment made by the Governor General, or by a Minister, otherwise than under a Commonwealth enactment; or</p>	<p>(e) a person holding or performing the duties of an office established by or under, or an appointment made under, a law of a State or Territory, other than the office of head of a State or Territory Department (however described)</p> <p>(f) a person holding or performing the duties of an appointment made, otherwise than under a law of a State or Territory, by:</p> <p>(i) a Governor of a State; <i>or</i>...</p> <p>(v) a State or Territory Minister; or</p>	
<p>(e) a local authority Sch 4 "local authority" means a council or county council within the meaning of the <i>Local Government Act 1993</i>.</p>			<p>(f) a local government authority</p>
<p>(f) a court Sch 4 cl 1</p> <p>(a) a tribunal, a Magistrate and a coroner, and</p> <p>(b) a registry or other office of a court and the members of staff of that registry or other office</p>	<p>(g) a federal court</p> <p>See (c) above.</p>	<p>(g) a State or Territory court</p>	<p>d) a person or body in relation to whom, or to whose functions, an account is kept of administration or working expenses, if the account: ...</p>

GIPA Act – agency (s 4)	Privacy Act (Cth) – agency (s 6)	Privacy Act (Cth) – State and Territory authority (s 6C)	PPIPA (s 3)
<p>(g) a person or entity that is an agency pursuant to regulations under clause 5 of Schedule 4</p> <p>Sch 4 cl 5 (1) The regulations may declare a person or entity that is not otherwise an agency to be an agency (a deemed agency) for the purposes of all or specified provisions of this Act and the <i>Government Information (Information Commissioner) Act 2009</i> in relation to all or specified agency functions of the person or entity.</p> <p>(2) A function of a person or entity is an agency function if it is:</p> <p>(a) a function of a kind that is or was ordinarily exercised by an agency, or</p> <p>(b) a function of an agency that the person or entity is exercising pursuant to a contract or other arrangement with the agency...</p>			



**Appendix B:  
Analysis of privacy  
codes of practice**

Name of privacy code	Agencies exempted	Privacy principles exempted	Analysis
Privacy Code of Practice (General) 2003 Part 2 – Inter-agency transfers of information	Roads and Traffic Authority, Environmental Protection Agency, Attorney General's Department (now the Department of Justice and Attorney General).	"IPPs are modified to the extent necessary to permit the transfer of information between the agencies" – s 9, 17, 18.	Covered to the extent necessary by UPP 5.1(f)(i), (iv), or by UPP 5.1(c) in the case of an environmental warning.
Privacy Code of Practice (General) 2003 Part 3 – Public registers	Various agencies who are responsible for keeping certain public registers.	Excluded from application of Part 6.	See chapter 8 (public registers).
Privacy Code of Practice (General) 2003 Part 4 – Human Services	Public sector agencies that provide any one or more of the following types of services to the public:  (a) welfare services, (b) health services, (c) mental health services, (d) disability services, (e) drug and alcohol treatment services, (f) housing and support services, (g) education services.	a) Sections 8-11, 17-19, where a "senior officer" has given authorisation. A senior officer must only give authorisation if he/she is satisfied that the related individual is or is proposed to receive services from an HSA, that the consent of the related individual or person authorised to give consent on that individual's behalf cannot or has not been given, there are reasonable grounds to believe that there is a "risk of substantial adverse impact" to that individual or others if the information is not collected, used or disclosed, that the information will be used to alleviate this risk and that all reasonable steps have been taken to notify the individual of the nature of the authorisation given.  b) Section 9, where unreasonable or impracticable.  There is an associated Code made under HRIPA exempting agencies from HPPs 3, 4, 10 and 11 in the same situations.	a) Covered by UPP 2.3(b), UPP 5.1(a) and (c). Note "risk of substantial adverse impact" is more general than "a serious threat to an individual's life, health or safety".  b) Covered by UPP 2.3(b).
Privacy Code of Practice (General) 2003 Part 5 – Corrective Services	Department of Corrective Services.	a) Section 9, where the collection is from NSW Police or CrimTrac relating to a criminal charge or conviction against a staff member affecting their suitability for employment, or relating to an AVO against an offender.  b) Section 9, where indirect collection is reasonably	a) UPP 2.3(b). Note proposed removal of s 4(3)(j). There may be situations covered by this Part that are not covered under UPP 2.3(b), such as where it is reasonable to ask a staff member



Name of privacy code	Agencies exempted	Privacy principles exempted	Analysis
		<p>necessary to protect or provide services to an offender, to maintain the security of a correctional or transitional centre, to verify information, to organise a conference or mediation or to investigate a misconduct allegation.</p> <p>c) Sections 10, 11(b), 13, 17 where reasonably necessary to do so to protect an individual, provide services to an offender, maintain the security of a correctional or transitional centre, exercise the complaint handling or investigative functions of the Department or carry out proceedings before or prepare a report to a court, tribunal or other related body.</p> <p>d) Sections 10, 13, 17 where it is reasonably necessary to prevent disclosure of intelligence information, the identity of an informant or victim, or the existence of a surveillance operation. Section 17 where it is necessary to organise a conference or mediation between offender and victim.</p> <p>e) Section 15, where the information relates to an ongoing investigation and it would prejudice the Department's complaints handling or investigative functions, provided that the information will be amended following the investigation.</p> <p>f) Sections 18 and 19 where the disclosure is necessary to protect or provide services to an individual or offender, to permit the Department of Human Services, the Department of Health or Justice Health to exercise its functions properly in relation to an offender, or to verify or obtain professional or technical advice about the information.</p>	<p>whether they have a criminal charge or conviction before then confirming with NSW Police or CrimTrac.</p> <p>b) The qualifier "reasonably necessary" means that the same criteria will apply under UPP 2.3(b).</p> <p>c) Covered by UPP 2.2 (no longer a reference to the extent of the intrusion, but the method of the collection), reasonableness qualifier in UPP 3, UPP 5.1 (c), (d), (f). Section 13 has no strict equivalent under the UPPs.</p> <p>d) Section 13 has no strict equivalent under the UPPs. There is thus no need to exempt from it. This exemption is otherwise covered by the reasonableness exemptions in UPP 3 and UPP 5.1(f).</p> <p>e) Covered by the reasonableness exemption in UPP 9.6, but note the requirements in UPP 9.7 and 9.8.</p> <p>f) Covered by UPP 5.1(c), and UPP 5.1(a).</p>

Name of privacy code	Agencies exempted	Privacy principles exempted	Analysis
Privacy Code of Practice (General) 2003 Part 6 – Ageing, Disability and Homecare Services	Department of Ageing, Disability and Homecare Services (now the Department of Human Services), the Home Care Service of NSW, the Disability Council of NSW.	<p>a) Provides that collection for the purposes of providing services to an individual is also undertaken to ensure the provision of appropriate services, to ascertain the appropriate priority or placement of an individual in a service, to prevent harm to the individual or others, and to ensure compliance with OHS laws by the agency.</p> <p>b) Where an individual lacks capacity, their “personal information custodian” (defined in sch 3) can exercise their functions under PPIPA for them.</p>	<p>a) Covered by UPP 5.1(a), but also raises the issue of “sector-specific” interpretation through privacy codes.</p> <p>b) See chapter 3 (consent).</p>
Privacy Code of Practice (General) 2003 Part 7 – Registry of Births, Deaths and Marriages	Registry of Births, Deaths and Marriages.	Exempts the Registry from collection, use, and disclosure IPPs where the information is collected, used or disclosed for the purposes of verifying or validating personal information for the Document Verification Service or the Certificate Validation Service.	May be covered by reasonableness exemptions under UPP 2.3(b), UPP 5.1(a).
Privacy Code of Practice for the Bureau of Crime Statistics and Research	Bureau of Crime Statistics and Research, other public sector agencies insofar as they disclose personal information to BOCSAR.	Sections 9, 10, 13, 15 if compliance would detrimentally affect or prevent the exercise by the Bureau of its functions.	Covered by the reasonableness requirements in UPP 2.3(b), UPP 3 and UPP 9.6. No equivalent for s 13 in the UPPs.

Name of privacy code	Agencies exempted	Privacy principles exempted	Analysis
The Privacy Code of Practice for the NSW Public Sector Workforce Profile	The Commissioner for Public Employment and delegates in the Department of Premier and Cabinet (previously the Premier's Department) and the Department of Services, Technology and Administration (previously the Department of Commerce).	<ul style="list-style-type: none"> <li>a) Exemption from s 9 insofar as the Commissioner gathers information from agencies that are not "public sector agencies" for the purposes of the Act (eg State owned corporations).</li> <li>b) Section 18 insofar as disclosure by the Premier's Department to the Department of Commerce is necessary for monitoring and development of the Shared Corporate Services Strategy. Section 19 to the extent that disclosure is not authorised by specific exemptions.</li> </ul>	<ul style="list-style-type: none"> <li>a) Exemption from s 9 covered by proposed change in definition of "public sector agency", and to any further extent covered by UPP 2.3(b) or by the research exemption in UPP 2.5(f).</li> <li>b) Sections 18 and 19 exemptions covered by the research exemption in UPP 5.1(g).</li> </ul> <p>The Workforce Profile relies generally upon the consent of the public sector employees giving their own personal information, and on the disclosure of information in a statistical, de-identified form.</p>
Privacy Code of Practice for Local Government	Councils and county councils as defined by the <i>Local Government Act 1993</i> .	<ul style="list-style-type: none"> <li>a) Sections 9, 10, 17 and 18 where the collection is for the purpose of conferring a prize or benefit on an individual.</li> <li>b) Section 17 where the use or disclosure is in pursuance of the Council's lawful and proper functions and the Council is satisfied that the personal information is reasonably necessary for the exercise of those functions.</li> <li>c) Section 18 where the disclosure is to another agency where the agency has approached the Council in writing and the Council is satisfied that the personal information is to be used for the lawful and proper functions of that agency and is reasonably necessary to do so.</li> <li>d) Section 18 where it is disclosed to a potential employer of a current or former Council employee, and the information disclosed is limited to the fact that they work or have worked for the Council, the duration and the position of that employment.</li> </ul>	<ul style="list-style-type: none"> <li>a) Covered by the reasonableness exemptions in UPP 2.3(b), UPP 3 and UPP 5.1(a). See section on s 26(1) PPIPA.</li> <li>b) Covered partly by UPP 5.1(a). The exemption as it stands is too broad. If there is doubt about whether it is a related use consent of the individual should be obtained.</li> <li>c) See above (b). The other agency should, where possible, collect information directly from the individual, or ask for the individual's consent for Council disclosure.</li> <li>d) Covered by UPP 5.1(a).</li> </ul>

Name of privacy code	Agencies exempted	Privacy principles exempted	Analysis
Privacy Code of Practice for the Office of the Director of Public Prosecutions	Office of the Director of Public Prosecutions.	Full exemption from s 13, and partial exemption from s 18 insofar as it is necessary to disclose information to the Victims Compensation Tribunal pursuant to s 30(1) of the <i>Victims Support and Rehabilitation Act 1996</i> (NSW) (previously the <i>Victims Compensation Act 1996</i> ).	Section 13 has no equivalent in the UPPs, and the s 18 exemption will be covered by UPP 5.1(e). The Victims Compensation Tribunal and the compensation assessor have power under s 60 and s 65A of the <i>Victims Support and Rehabilitation Act 1996</i> (NSW) respectively.
Privacy Code of Practice for the NSW Department of Education and Training	Department of Education and Training.	<ul style="list-style-type: none"> <li>a) Investigative functions: Exemption from all IPPs except s 8, 11, 16.</li> <li>b) "Safe and disciplined learning environment": Exemption from all IPPs except s 8, 11, 12, 16. This phrase refers to the Minister for Education's power under s 35(1) of the <i>Education Act 1991</i> to "control and regulate student discipline in government schools" interpreted in the <i>Ministerial Statement on Good Discipline and Effective Learning</i> (1995), now the <i>Student Discipline in Government Schools Policy</i> (2006).</li> <li>c) Parent, guardian, caregiver: Modifies s 9, 10, 14, 15, 17-19 to allow a parent, guardian or caregiver to stand in place of a student. Where this relates to sensitive information, it must be in the best interests of the child.</li> <li>d) Counsellor records: Modifies s 13 and 15 to disallow access or correction of personal information when contained in counsellor records.</li> <li>e) Child protection: Exemption from s 17-19 where the use or disclosure is for child protection purposes.</li> <li>f) Legal purposes: Exemption from s 17-19 where the use or disclosure is for the purpose of obtaining legal advice or for use in legal proceedings.</li> <li>g) Board of Studies: Exempts from s 18 where disclosure is to the Board of Studies for the purpose of the School Certificate or the Higher School Certificate.</li> </ul>	<ul style="list-style-type: none"> <li>a) Covered by UPP 5.1(d).</li> <li>b) These exemptions would be covered by the reasonableness and "required or authorised by law" provisions in UPPs 2.3(b), 2.5(b), 3 and 5.1(e). The Minister has power to obtain information from various agencies under the <i>Education Act 1991</i> (NSW) div 2 and the power to issue binding guidelines (which are "law" for the purposes of "required or authorised by law" exemptions – see chapter 4) under Division 4. Specifically, the Minister has the power to "control and regulate student discipline in government schools" under s 35(1).</li> <li>c) See chapter 3 (consent).</li> <li>d) No equivalent to s 13, covered by reasonableness requirement in UPP 9.6.</li> <li>e) Covered by UPP 5.1(a), (c), (f).</li> </ul>

Name of privacy code	Agencies exempted	Privacy principles exempted	Analysis
			<p>f) Covered by UPP 5.1(f)(v), (h).</p> <p>g) Covered by reasonableness provision in UPP 5.1(a) – use for the School Certificate or Higher School Certificate is related, if not directly related, to the primary purpose of collection.</p>
<p>Privacy Code of Practice for the NSW Police Service</p>	<p>NSW Police Service.</p>	<p>a) Exemption from s 9, 17 and 18 where the collection, use or disclosure of information is with the Roads and Traffic Authority in regard to motor vehicle accidents and other traffic related data, or with the National Motor Vehicle Theft Reduction Council, particularly with regard to the Comprehensive Auto-Theft Research System database.</p> <p>b) Exemption from s 18 where disclosure is to Housing NSW (previously the Department of Housing) relating to a complaint about a tenant and the personal information held is directly relevant to that investigation, or where a possible offence may be in breach of a Housing NSW tenancy agreement.</p> <p>c) Exemption from s 18 where disclosure of a motor accident or crime incident report is to an insurer where a claim has been lodged against that insurer and the report is related to that claim.</p> <p>d) Exemption from s 18 where disclosure of a motor accident report is to an individual to whom that report relates.</p> <p>e) Exemption from s 18 where the Police Service allows the Police Association of NSW to access the "POL" function of the Eagle mainframe system to obtain member, work location, contact and rank details.</p>	<p>a) This would be covered by the reasonableness exemptions under UPP 2.3(b) and UPP 5.1(a), or perhaps the research exemptions under UPP 2.5(f) and UPP 5.1(g). The Code could go into more detail about what kind of information is exchanged, and whether it is or could be made de-identifiable.</p> <p>b) This would be covered by UPP 5.1(f), as "enforcement body" would cover NSW Police and Housing NSW in its responsibility for administering a law that imposes a penalty or sanction or a prescribed law.</p> <p>c)-e) All these would be covered by the reasonableness exemption in UPP 5.1(a), or the enforcement body exemptions in UPP 5.1(f).</p>

Name of privacy code	Agencies exempted	Privacy principles exempted	Analysis
Privacy Code of Practice for the Department of Housing	Housing NSW (previously the Department of Housing)	<p>a) Exemption from s 9 for the Priority Housing Assistance Program where disclosure of personal information by other agencies or individuals (health professionals, NGOs) is permitted by law, and where it is impracticable to collect the information directly or to gain the individual's consent.</p> <p>b) Exemption from s 9 for individuals under the age of sixteen – Dept can collect information from third parties other than parent/guardian where this is in the best interests of the child.</p> <p>c) Exemption from s 9, 10, 13 relating to investigative or complaints handling functions.</p> <p>d) Exemption from s 9 where information is collected from Community Housing Organisations funded by the Office of Community Housing for the purposes of providing services or aid to community housing applicants or tenants, or for receiving complaints or appeals.</p> <p>e) Exemption from s 9 and 17 where an appeal is made to the Housing Appeal Committee. The individual who made the appeal is taken to consent to the referral of all relevant documents to the HAC for the purposes of hearing the appeal. Notification requirements under s 10 still apply.</p> <p>f) Exemption from s 9 where information is collected from loan managers or FANMAC Ltd in respect of individuals who hold or held government home loans, for the purposes of managing home purchase assistance schemes. Section 10 still applies.</p> <p>g) Exemption from s 9 where, for the purposes of managing Residential Tenancy Agreements, HPAA collects personal information from Public Housing.</p>	<p>a) UPP 2.3(b), but Code is useful here for clarification.</p> <p>b) Covered by reasonableness provision in UPP 2.3(b).</p> <p>c) Covered by the reasonableness provisions in UPP 2.3(b) and UPP 3.</p> <p>d) Covered by the reasonableness provision in UPP 2.3(b).</p> <p>e) UPP 2.3(b), UPP 5.1(a), (h).</p> <p>f) UPP 2.3(b).</p> <p>g) UPP 2.3(b).</p> <p>h) UPP 5.1(a).</p> <p>i) This list would be "open access information" under s 18(e) of the not yet commenced <i>Government Information (Public Access) Act 2009</i> (NSW). Alternatively, the contractor should be notified of the potential disclosure of this information before collection. The disclosure would then be covered by UPP 5.1(a).  The public register provisions under Part 6 would also apply to this. See the "public registers" section of the report.</p>

Name of privacy code	Agencies exempted	Privacy principles exempted	Analysis
		<p>h) Exemption from s 18 where disclosure is to the Aboriginal Housing Office or the Community Housing Office or relevant Community Housing Organisation for Aboriginal Housing or Community Housing purposes.</p> <p>i) Exemption from s 18 with respect to successful contractors – the name of the contractor and the amount tendered.</p>	
Privacy Code of Practice for the Legal Aid Commission	Legal Aid Commission.	Exemption from s 9 and 10 with respect to the collection of personal information relating to financially associated persons and dependants for the purposes of determining eligibility for legal aid.	Covered by the reasonableness requirements in UPP 2.3(b), but the Code is useful in clarifying the process by which the personal information is collected.
Privacy Code of Practice for the Department of Fair Trading	NSW Fair Trading (previously the Department of Fair Trading).	<p>a) Exemptions from all IPPs except s 8, 11, 12, 16 where it is reasonably necessary for the proper functioning of the Department's complaints handling, investigative or law enforcement functions. These functions also include, broadly, licensing and certification activities of the Department.</p> <p>b) Exemption from s 9 where letters containing personal information are referred on to the Department from other agencies.</p>	<p>a) Covered by UPP 5.1(f) as the Department of Fair Trading will be included as an "enforcement body".</p> <p>b) This would be covered by UPP 2.3(b). See also UPP 2.4 on unsolicited information and the analysis of that in CP 3, [2.48]-[2.80]</p>





**Appendix C:  
Analysis of public  
interest directions**

\* For reasons of space, a full list of named agencies is sometimes not given. That full list is contained in a schedule to each public interest direction and can be accessed at the Privacy NSW website.

Name of public interest direction	Agencies exempted*	Starting date and Number of renewals	IPPs exempted	Analysis
Direction relating to requests made by the Ombudsman under section 13AA of the <i>Ombudsman Act 1974</i>	All NSW public sector agencies.	23 December 2008. Renewed twice.	Sections 16, 17, 18, 19(1) where a request is made by the Ombudsman under s13AA of the <i>Ombudsman Act 1974</i> (NSW).	Covered by UPP 5.1(d)-(f) in conjunction with s 18 of the <i>Ombudsman Act 1974</i> (NSW). Proposed inclusion of provision in <i>Ombudsman Act</i> similar to the <i>Ombudsman Act 1976</i> (Cth) s 7A(1D).
Direction relating to the Anti-Social Behaviour Pilot Project	Health, Housing, Youth, Human and Corrective Services, the NSW Police Force, Premier's Department and the Department of Aboriginal Affairs.	2 September 2008. Operative until the completion of the ASBPP.	Sections 8(1), 9, 10, 17-19, where exemption is reasonably relevant and reasonably necessary for the purpose of meeting the objects of the ASBP Project. There is an associated PID under HRIPA granting exemption from HPPs 3, 4, 10 and 11.	Covered by reasonableness provisions in UPP 2.3(b) and by UPP 5.1(c) or (f). Outlines need for retention of Privacy Codes in order to interpret or provide specific guidance on UPPs.
Direction relating to the Document Verification Service NSW Registry of Births, Deaths and Marriages	The NSW Registry of Births, Deaths and Marriages in its administration of the Document Verification Service.	9 July 2009. Completed. This direction is no longer valid (as of 9 January 2010) and is only included for reference purposes.	Sections 9-11, 17, 18.	Arguably covered by UPP 5.1(a) and (b) and UPP 2.3(a). See also analysis of General Code.

Name of public interest direction	Agencies exempted*	Starting date and Number of renewals	IPPs exempted	Analysis
Direction relating to the Child Protection Watch Team Trial	NSW Police, Department of Community Services, Department of Corrective Services, Department of Juvenile Justice, Department of Ageing, Disability and Home Care, Department of Health, Department of Housing, Department of Education and Training, Sydney South West Area Health Service.	7 Aug 2006. Operative until the completion of the CPWTT.	All sections except s 11, 12, 16, for the purposes of the CPWT Trial and as long as disclosure is within the named agencies.	Covered by reasonableness provisions generally and by UPP 5.1(c), (d), or (f).
Direction relating to the Redfern Waterloo Partnership Project	Same as above with the inclusion of the Premier's Department, the Department of Aboriginal Affairs and the Redfern-Waterloo Authority.	2 Feb 2006. Operative until the completion of the RWPP.	Sections 8(1), 9, 10, 17-19, where exemption is reasonably relevant and reasonably necessary for the purpose of meeting the objects of the Redfern-Waterloo Partnership Project. There is an associated PID under HRIPA granting exemption from HPPs 3, 4, 10 and 11.	Covered by reasonableness provisions in UPP 2.3(b) and by UPP 5.1(c) or (f). Again, guidelines or codes could be used to interpret the requirements of the privacy principles.
Direction relating to the Collection of Personal Information about Third Parties by NSW Public Sector (Human Service) Agencies from Their Clients	Some health, education, welfare, housing, juvenile justice and Aboriginal affairs agencies.	26 June 2003. Renewed 7 times.	Sections 9 and 10.	Covered by reasonableness exemption in UPP 2.3(b).

Name of public interest direction	Agencies exempted*	Starting date and Number of renewals	IPPs exempted	Analysis
Direction relating to the Disclosures of Information by the NSW Public Sector Agencies to the National Coronial Information System (NCIS)	All NSW public sector agencies.	18 February 2002. Renewed 10 times.	Sections 18 and 19(1), for the purposes of disclosure to the NCIS.	Covered by research exemption in UPP 5.1(g), or by reasonableness exemption in UPP 5.1(a).
Direction relating to the Disclosures of Information by NSW Public Sector Agencies for Research Purposes	Most NSW public sector agencies, including councils, universities, departments, trusts, tribunals, commissions, boards, art galleries and museums.	30 June 2000. Renewed 15 times.	<p>Sections 18 and 19 where information is disclosed for the purposes of research, provided prescribed guidelines are followed or approval has been given by an ethics committee.</p> <p>Reasonable departure from all sections except s 11 and 12 where information is held for purposes including research.</p> <p>All sections except s 11-13 and 16 where the information is of historical or cultural significance and is held for reference purposes.</p>	Covered by research exemptions in UPP 2.5(f), 5.1(g) and 9.6.
Direction relating to the Disclosure of Information to Victims of Crime	Law enforcement, health and justice agencies.	30 June 2000. Renewed 15 times.	Sections 9, 10, 17-19 where necessary to give effect to the <i>Victims Rights Act 1996</i> (NSW) or the <i>Victims Support and Rehabilitation Act 1996</i> (NSW).	Covered by UPP 2.3(b), UPP 3 and UPP 5.1(e). This disclosure is "required or authorised by law" pursuant to s 7 of the <i>Victims Rights Act 1996</i> .
Direction relating to the Department of Ageing, Disability and HomeCare and Associated Agencies	Department of Ageing, Disability and Homecare, Guardianship Tribunal, Disability Council.	16 March 2001. Renewed 13 times.	Modification of s 9, 14, 15, 17-19 to provide for substitute consent.	See chapter 3 (consent).

Name of public interest direction	Agencies exempted*	Starting date and Number of renewals	IPPs exempted	Analysis
Direction relating to the Processing of Personal Information by NSW Public Sector Agencies in relation to their Investigative Functions	All NSW public sector agencies.	28 September 2000. Renewed 15 times.	All sections except s 8, 11, 12 and 16, where reasonably necessary for the proper exercise of an agency's investigative functions or in the conduct of a lawful investigation.  Sections 18 and 19(1) where disclosure is reasonably necessary to assist another agency in the above functions.	Covered by UPP 5.1(d). See investigative agencies section of report for further analysis.
Direction relating to the Information Transfers between NSW Public Sector Agencies	All NSW public sector agencies.	30 June 2000. Renewed 16 times.	Exempts exchanges of information from all sections where reasonably necessary:  a) to allow agencies to deal with or respond to correspondence from Ministers or MPs;  b) for the purposes of referring inquiries between agencies;  c) for auditing purposes; or  d) for law enforcement purposes not covered by Part 2, Division 3.	Exemptions (a)-(c) are covered where necessary by the reasonableness exemptions in UPP 2.3(b) and UPP 5.1(a). For exemption (a), see chapter 6.  d) Law enforcement purposes are covered by the proposed UPPs. See chapter 5.



**Appendix D:  
Submissions and  
consultations**

Office of the Privacy Commissioner, 13 October 2008  
Justice Health, NSW Health, 15 October 2008  
NSW Commission for Children and Young People, 15 October 2008  
NSW Department of Primary Industries, 15 October 2008  
Motor Accidents Authority of NSW, 16 October 2008  
Australian Press Council, 17 October 2008  
Legal Aid NSW, 17 October 2008  
NSW Department of Corrective Services, 17 October 2008  
Business Law Committee of the Law Society of NSW, 21 October 2008  
Office of Fair Trading, NSW Department of Commerce, 22 October 2008  
State Records Authority of NSW, 23 October 2008  
NSW FOI/Privacy Practitioners' Network, 28 October 2008  
NSW Department of Ageing, Disability and Home Care, 30 October 2008  
NSW Department of Community Services, 30 October 2008  
Australian Privacy Foundation, 31 October 2008  
Cyberspace Law and Policy Centre, University of NSW, 3 November 2008  
HIV/AIDS Legal Centre, 4 November 2008  
Intellectual Disability Rights Service, 5 November 2008  
Office of Industrial Relations, NSW Department of Commerce,  
7 November 2008  
Inner City Legal Centre, 10 November 2008  
Consumer Credit Legal Centre (NSW) Inc, 13 November 2008  
NSW Guardianship Tribunal, 17 November 2008  
Privacy NSW, Office of the NSW Privacy Commissioner,  
28 November 2008  
Public Interest Advocacy Centre Ltd, 24 December 2008  
NSW Department of Education and Training, 2 February 2009  
Crime Prevention Division, NSW Department of Justice and Attorney  
General, 19 January 2010  
NSW Ombudsman, 12 March 2010



**Appendix E:  
Preliminary  
submissions**

Council of Social Services of NSW, 2 January 2006  
National Health and Medical Research Council, 2 June 2006  
NSW Office of the Protective Commissioner, 4 July 2006  
NSW Department of Local Government, 9 June 2006  
NSW Department of Community Services, 14 June 2006  
Australian Broadcasting Corporation, 23 June 2006  
Casino Control Authority, 28 June 2006  
State Records Authority of NSW, 31 July 2006  
The Royal Australian College of General Practitioners NSW  
and ACT Faculty, 7 July 2006  
Sydney Opera House, 9 July 2006  
Powerhouse Museum, 26 July 2006  
Legal Aid NSW, 26 July 2006  
State Library of NSW, 28 July 2006  
Art Gallery of NSW, 31 July 2006  
Law Society of NSW, 31 July 2006  
NSW Office of Fair Trading, 1 August 2006  
NSW Department of Arts, Sport and Recreation, 7 September 2006  
NSW Health, 18 September 2006  
NSW FOI/Privacy Practitioners' Network, 25 September 2006  
Public Interest Advocacy Centre and Shopfront Youth Legal  
Centre, 17 October 2006  
Shopfront Youth Legal Centre, 17 October 2006  
NSW Department of Commerce, 4 October 2006  
NSW Department of Housing, 5 October 2006  
Miss Noelle Sertori, 14 November 2006  
NSW Mental Health Review Tribunal, 20 November 2006

# Tables

- Table of cases
- Table of legislation

---

**Table of cases**


---

<i>Applicant VEAL of 2002 v Minister for Immigration and Multicultural and Indigenous Affairs</i> (2005) 225 CLR 88 .....	4.30
<i>AT v Commissioner of Police, New South Wales Police Force</i> [2009] NSWADTAP 1.....	12.25
<i>Attorney-General (Cth) v Breckler</i> (1999) 197 CLR 82 .....	7.52
<i>Attorney-General for New South Wales v Nationwide News Pty Ltd</i> (2007) 72 NSWLR 635 .....	6.7
<i>BQ v Commissioner of Police, New South Wales Police Service</i> [2002] NSWADT 64 .....	12.22
<i>BY v Director General, Attorney General's Department (No. 2)</i> [2003] NSWADT 37 .....	5.7
<i>Brennan and the Law Society of the Australian Capital Territory, Re</i> (1984) 6 ALD 428 .....	2.13, 2.14
<i>CP v NSW Ombudsman</i> [2002] NSWADT 103 .....	2.54
<i>Caratti v Commissioner of Taxation</i> (1999) 99 ATC 5044.....	4.16
<i>Channel 31 Community Educational Television Ltd v Inglis</i> (2001) 25 WAR 147 .....	2.13
<i>Commissioner of Police, New South Wales Police Force v YK</i> [2008] NSWADTAP 78 .....	5.58, 5.68
<i>Commonwealth v Northern Land Council</i> (1993) 176 CLR 604 .....	11.16, 11.26
<i>D (Minors), In Re</i> [1993] Fam 231 .....	4.30
<i>Daniels Corporation International Pty Ltd v Australian Competition and Consumer Commission</i> (2002) 213 CLR 543.....	11.16
<i>Department of Education and Training v GA (No 3)</i> [2004] NSWADT 50.....	12.9
<i>Director General, Department of Education and Training v MT</i> (2006) 67 NSWLR 237 .....	4.30, 9.57
<i>Director General, Department of Education and Training v MT</i> [2005] NSWADTAP 77 .....	4.18

<i>DPP v Ritson</i> (Local Court, Magistrate Bartley, 12 February 2009) .....	6.7, 9.52
<i>DPP v Ritson</i> (Local Court, Magistrate Bartley, 7 April 2009).....	9.52
<i>EG v Commissioner of Police</i> [2004] NSWADTAP 10.....	8.4
<i>Environment Protection Authority v Caltex Refining Co Pty Ltd</i> (1993) 178 CLR 477 .....	11.16
<i>FM v Vice Chancellor, Macquarie University</i> [2003] NSWADT 78.....	6.25, 12.33
<i>Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW</i> [2003] NSWADT 132 .....	12.21, 12.22
<i>GA v Department of Education and Training</i> [2005] NSWADT 47 .....	12.8
<i>GA v Department of Education and Training</i> [2004] NSWADTAP 18.....	6.51
<i>GA v Department of Education and Training</i> [2005] NSWADTAP 64.....	12.8
<i>GQ v NSW Department of Education and Training</i> [2008] NSWADT 212.....	12.23
<i>GV v Office of the Director of Public Prosecutions</i> [2003] NSWADT 177.....	4.18, 7.53
<i>Greig v University of Edinburgh</i> (1866) LR 1 Sc & D 348 .....	2.13
<i>HW v Commissioner of Police, New South Wales Police Service</i> [2003] NSWADT 214 .....	4.18, 5.55, 5.59-5.60, 5.68
<i>Hancock v Birsa</i> [1972] WAR 177 .....	7.53
<i>JD v Department of Health</i> [2005] NSWADTAP 44.....	5.7
<i>JD v NSW Medical Board</i> [2005] NSWADT 247 .....	5.7
<i>JW v Pittwater Council</i> [2009] NSWADT 4 .....	12.22
<i>John Fairfax Publication Pty Ltd v District Court of New South Wales</i> (2004) 61 NSWLR 344 .....	6.5, 6.7
<i>John Fairfax Publication Pty Ltd v Ryde Local Court</i> (2005) 62 NSWLR 512 .....	6.5
<i>JS v Snowy River Shire Council (No 2)</i> [2009] NSWADT 210 .....	4.17
<i>KD v Registrar, NSW Medical Board</i> [2004] NSWADT 5.....	4.18, 4.30

<i>KO v Commissioner of Police, NSW Police</i> [2004] NSWADT 3 .....	11.33, 12.8
<i>KO v Commissioner of Police</i> [2004] NSWADTAP 21 .....	6.51
<i>Kioa v West</i> (1985) 159 CLR 550.....	4.30
<i>Magdalen College Case</i> (1615) 11 Co Rep 66b .....	11.8
<i>McGuinness v Attorney General (Vic)</i> (1940) 63 CLR 72.....	6.11
<i>McNamara v Consumer Trader and Tenancy Tribunal</i> (2005) 221 CLR 646.....	2.6
<i>Melbourne Harbour Trust Commissioners v Colonial Sugar Refining Company Ltd</i> (1925) 36 CLR 230 .....	11.8
<i>Mersey Docks and Harbour Board Trustees v Cameron</i> (1865) 11 HL Cas 443 .....	2.13
<i>Minister for Urban Affairs and Planning v Rosemount Estates</i> (1996) 91 LGERA 31.....	1.20
<i>MT v Director General, NSW Department of Education and Training</i> [2004] NSWADT 194.....	4.18
<i>Municipal Association of Victoria v Victorian Civil and Administrative Tribunal</i> [2004] VSC 146 .....	2.13-2.15
<i>NR v Roads and Traffic Authority</i> [2004] NSWADT 276.....	12.8
<i>NW v NSW Fire Brigades</i> [2005] NSWADT 73.....	5.17
<i>NZ v Director General, Attorney General's Department</i> [2005] NSWADTAP 62 .....	6.4, 6.10
<i>NZ v Attorney General's Department</i> [2005] NSWADT 103.....	6.4, 6.8, 6.10
<i>NSW Bar Association, Re An Application by the</i> [2004] FMCA 52....	4.18, 7.53
<i>NSW Grains Board, Re: Smith v Lawrence</i> (2002) 171 FLR 68.....	2.17
<i>ON v Marrickville Council</i> [2005] NSWADT 274 .....	12.9
<i>OQ v Commissioner of Police</i> [2005] NSWADT 240 .....	5.60
<i>PC v University of New South Wales</i> [2005] NSWADTAP 72 .....	9.6
<i>PC v University of New South Wales (No 2)</i> [2005] NSWADT 264.....	12.21, 12.22
<i>PC v University of New South Wales (No 2)</i> [2006] NSWADTAP 54.....	12.22

<i>Queensland Law Society Inc v Albietz</i> [1996] 2 Qd R 580 .....	2.13
<i>Rahman v Ashpole</i> [2007] FCA 1067.....	4.16
<i>Renmark Hotel Inc v Federal Commissioner of Taxation</i> (1949) 79 CLR 10.....	2.13
<i>Richards v State of Victoria</i> [1969] VR 136 .....	4.30
<i>Roddan v Walker</i> (1997) 94 A Crim R 170 .....	7.53
<i>SZBEL v Minister for Immigration and Multicultural and Indigenous Affairs</i> (2006) 228 CLR 152 .....	4.30
<i>Secretary to the Department of Premier and Cabinet v Hulls</i> [1999] 3 VR 331 .....	4.16
<i>Sweeney v Boylan Nominees</i> (2006) 227 ALR 46.....	2.46
<i>Vice-Chancellor Macquarie University v FM</i> [2005] NSWCA 192.....	12.33
<i>Vice-Chancellor, Macquarie University v FM</i> [2003] NSWADTAP 43 .....	6.25, 12.33, 12.37
<i>Vice-Chancellor, Macquarie University v FM (No.2)</i> [2004] NSWADTAP 37 .....	12.33
<i>Western Australian Turf Club v Federal Commissioner Of Taxation</i> (1978) 19 ALR 167.....	2.14
<i>Wilson v McDonald</i> (2009) 253 ALR 560 .....	7.53
<i>Wood v State of NSW</i> [2008] FMCA 566.....	2.55, 2.56
<i>Workcover Authority of NSW (Inspector Keelty) v The Crown in Right of the State of NSW (Police Service of NSW)</i> [2000] NSWIRComm 234 .....	11.8
<i>Worthing v Rowell</i> (1970) 123 CLR 89 .....	2.13
<i>Wykanak v Director General, Department of Local Government</i> [2002] NSWADT 208.....	12.9
<i>YK v Commissioner of Police, New South Wales Police</i> [2008] NSWADT 81.....	5.57
<i>ZR v NSW Department of Education and Training</i> [2009] NSWADT 84...	4.25
<i>ZR v NSW Dept of Education and Training</i> [2008] NSWADT 199 .....	12.8

## Table of legislation

---

### Commonwealth

#### *Constitution*

s 109 .....2.28

*Corporations Act 2001* .....2.17, 2.18, 2.27, 8.40

s 5A(1) .....11.8

#### *Freedom of Information Act 1982*

s 4 .....2.12

*Healthcare Identifiers Bill 2010* .....1.15

#### *Legislative Instruments Act 2003*

s 17-19 .....7.7

#### *Ombudsman Act 1976*

s 7A(1D) ..... 4.36-4.37

#### *Privacy Act 1988*

pt 3AA ..... **R 7.4**, 7.15

s 6 ..... 2.12, 2.26, 2.32, 2.45, 3.36, 5.22, 5.44

s 6C ..... 2.4, 2.29, 2.34

s 6C(3) .....2.4

s 6C(3)(a) .....2.8, 2.51

s 6C(3)(c) .....2.18

s 6C(3)(d) .....2.5

s 6C(3)(e) ..... 2.34-2.35

s 6C(3)(f) ..... 2.5, 2.34-2.35

s 6F ..... 2.4, 2.18-2.19, 2.23-2.24

s 7B(5) .....2.38

s 13, 13A .....11.35

s 18BB .....7.22

s 18BB(1) .....7.36



s 18BB(2)(a).....	7.26, 7.36
s 18BB(2)(f) .....	7.36
s 18BI .....	7.25
s 27(1)(a) .....	9.13, 11.45
s 27(1)(aa).....	7.25
s 27(1)(ab) .....	11.45
s 27(1)(ad) .....	7.25
s 27(1)(ae) .....	7.25
s 27(1)(c).....	10.8
s 27(1)(ea).....	7.25
s 27(1)(g) .....	10.10
s 27(1)(h) .....	10.13
s 30(1) .....	10.18
s 36(1) .....	11.35
s 36(2) .....	11.50
s 38(1)(c).....	11.50
s 38A, 38C .....	11.50
s 40(2) .....	10.17
s 41 .....	11.39
s 43(3) .....	11.13
s 44-46.....	11.13
s 49(1). .....	9.56
s 52(1)(b) .....	9.13
s 55A.....	9.14
s 61 .....	9.15
s 65-66.....	11.13
s 66(1B).....	11.23
s 68 .....	11.27
s 69-70.....	11.13

s 72 .....	7.91
s 72(2)(b) .....	7.82
s 72(5) .....	7.75
s 75 .....	7.82
s 79 .....	<b>R 7.5</b>
s 79(2) .....	7.82
s 79(3) .....	7.82, 7.87
s 80(1) .....	7.82
s 80 .....	7.90
s 80C .....	7.90
s 80E.....	7.82, 7.90
s 95B.....	2.45, 2.50
s 98 .....	10.25
s 100 .....	7.6
s 100(2) .....	7.7
sch 3 NPP 2.1(f), (h).....	5.28
sch 3 NPP 7.1A.....	7.7
sch 3 NPP 7.1.....	7.7
<i>Privacy (Private Sector) Regulations 2001.....</i>	2.19
<i>Privacy Amendment (Private Sector) Act 2000 .....</i>	1.21
<i>Privacy Amendment (Private Sector) Bill 2000 .....</i>	2.23
<i>Royal Commissions Act 1902 .....</i>	6.11

## New South Wales

### *Administrative Decisions Tribunal Act 1997*

s 7 .....	12.19
s 8 .....	12.19-12.21
s 37, s 38 .....	12.19
s 53 .....	12.21
s 63-66.....	9.4, 12.21, 12.28

s 75(2) .....	6.6
s 88(1) .....	12.21
s 88(3) .....	12.19, 12.21
s 112(1)(a).....	12.21
<i>Administrative Decisions Tribunal Amendment Act 2008</i>	
sch 1[1] .....	12.20-12.21
<i>Children and Young Persons (Care and Protection) Act 1998</i>	
s 27 .....	3.91
s 254.....	7.52
<i>Chiropractors Act 2001</i>	
sch 1 cl 21(3) .....	8.6
<i>Civil Liability Amendment (Privacy) Bill 2009 (Draft)</i>	
cl 72.....	1.26
<i>Community Welfare Act 1987</i>	
s 76 .....	7.52
<i>Conveyancing Act 1919</i> .....	8.10
<i>Coroners Act 1980</i> .....	6.3
<i>Court Information Bill 2009 (Consultation Draft)</i> .....	6.10
cl 16(1).....	6.9
<i>Crimes (Administration of Sentences) Act 1999</i>	
s 76 .....	7.52
<i>Freedom of Information Act 1989</i> .....	1.6, 2.22, 6.4, 8.16
s 7 .....	2.12
sch 1 cl 1-cl 2.....	11.5, 11.26
<i>Government Information (Information Commissioner) Act 2009</i>	
s 3 .....	7.62, 9.16

s 16.....	10.6
s 17.....	9.17
s 26.....	11.27
s 27(1).....	11.22
s 27(3).....	11.13
s 28.....	9.16
s 28(1)-(2).....	10.25
s 28(5).....	10.27
s 37.....	10.34
s 43(5).....	10.37
s 44.....	7.62
<i>Government Information (Public Access) (Consequential Amendments and Repeal) Act 2009</i> .....	8.16
<i>Government Information (Public Access) Act 2009</i> .....	1.6, 2.2, 5.41, 6.4, 8.16
pt 4 div 3.....	9.16
s 4.....	2.28, 2.35
s 4(1).....	2.5
s 4(1)(b).....	2.51
s 6(1).....	8.16
s 11.....	8.16
s 17(a).....	10.5
s 80.....	9.16
s 89.....	9.16
s 89(4).....	9.17
s 100.....	9.16
sch 4 cl 1.....	6.3, 11.12
sch 4 cl 2.....	2.12, 2.15
sch 4 cl 2(2).....	2.32
sch 4 cl 2(f).....	2.28

sch 4 cl 3 .....	2.35
sch 5 .....	2.32
sch 5 cl 3 .....	8.16
<i>Government Information (Public Access) Regulation 2009</i> .....	2.32
<i>Guardianship Act 1987</i> .....	3.39, 3.47, 3.55, 3.56
pt 5 .....	3.39
s 33A .....	3.43
sch 3 cl 3 .....	6.32
<i>Health Records and Information Privacy Act 2002</i> .....	<b>R 1.1</b> , 1.8, 1.11, 7.24
s 3 .....	1.21, 1.26
s 4 .....	3.10, 4.5, 5.4, 7.66
s 4(1) .....	2.1, 2.3
s 5 .....	4.1
s 5(3) .....	5.31
s 5(3)(j) .....	6.13
s 5(3)(k) .....	6.49, 6.51
s 5(3)(m) .....	6.44
s 6 .....	4.1
s 7 .....	3.9, 3.39, 3.54, 6.22, 7.48
s 8 .....	3.39, 3.77, 7.48
s 9(b) .....	3.77
s 11 .....	3.92
s 13 .....	<b>R 6.1-6.2</b> , 4.1, 6.2, 6.13
s 14 .....	4.1
s 17 .....	4.1, 5.54, 5.59, 5.62
s 21 .....	1.14, 9.12, 11.21
s 22 .....	4.1
s 22(3) .....	5.41
s 23 .....	4.15

s 24	10.28
s 28(2)	10.28
s 29	5.41, 10.28
s 42	9.12
s 43	9.12, 11.38
s 43(3)	11.42
s 44	9.12, 11.42
s 46	11.44
s 46(3)	9.45
s 47	10.14, 11.46, 11.48
s 48	9.12
s 48(1)	12.21
s 48(2)	12.23
s 50	10.14, 12.39
s 54	9.12, 12.27
s 55	9.12, 12.35
s 56	9.45, 12.27
s 57	12.37
s 58	10.3, 10.5
s 58(a)	10.9
s 58(b)	10.28
s 58(d)	10.8
s 58(e)	10.9, 10.14
s 59, 60	11.6
s 62	7.66
s 64	10.28
s 65-67	1.15, 11.40
s 68	9.45, 9.49, 9.60, 10.35
s 69	9.45, 9.49

s 70 .....	9.45, 10.35, 10.37
s 75 .....	7.4
sch 1 .....	4.1
sch 1 HPP 3.....	3.80, 7.46, 10.28
sch 1 HPP 4.....	3.10, 3.14, 6.24, 10.28
sch 1 HPP 4(4)(a) .....	6.24
sch 1 HPP 4(4)(b) .....	4.15, 4.19, 4.20
sch 1 HPP 4(4)(d).....	<b>R 6.4</b> , 6.21, 6.31
sch 1 HPP 4(4)(e) .....	5.5, 5.45
sch 1 HPP 4(4)(f) .....	5.5
sch 1 HPP 4(7) .....	5.5
sch 1 HPP 5(2)(a) .....	4.15, 4.19, 4.20
sch 1 HPP 5(3) .....	5.5
sch 1 HPP 6.....	4.24, 5.41
sch 1 HPP 6(2)(a) .....	4.15, 4.19, 4.20, 5.41
sch 1 HPP 7.....	5.41
sch 1 HPP 7(2)(a) .....	4.15, 4.19, 4.20, 5.41
sch 1 HPP 8.....	5.41
sch 1 HPP 8(4)(a) .....	4.15, 4.19, 4.20, 5.41
sch 1 HPP 10.....	3.11, 3.14, 6.24, 10.28
sch 1 HPP 10(1)(a) .....	6.24
sch 1 HPP 10(1)(f) .....	5.33
sch 1 HPP 10(1)(g) .....	5.5, 5.45
sch 1 HPP 10(1)(h)(ii) .....	5.5
sch 1 HPP 10(1)(i) .....	5.5, 5.45
sch 1 HPP 10(1)(j) .....	5.5, 5.6, 5.19, 5.49, 5.52
sch 1 HPP 10(2)(a) .....	4.15, 4.19, 4.20
sch 1 HPP 10(3) .....	<b>R 6.5</b> , 5.5, 6.32, 6.34-6.35
sch 1 HPP 10(4) .....	<b>R 6.6</b> , 6.36

sch 1 HPP 10(5) .....	5.5, 5.6, 5.15, 5.19, 5.50, 5.52
sch 1 HPP 11.....	3.11, 3.14, 6.24
sch 1 HPP 11(1)(a) .....	6.24
sch 1 HPP 11(1)(h) .....	5.5, 5.45
sch 1 HPP 11(1)(i) .....	5.16
sch 1 HPP 11(1)(j).....	5.5, 5.33, 5.45
sch 1 HPP 11(1)(k) .....	5.5-5.6, 5.11, 5.15, 5.19, 5.49, 5.52
sch 1 HPP 11(2)(a) .....	4.15, 4.19, 4.20
sch 1 HPP 11(2)(c) .....	5.5
sch 1 HPP 11(3) .....	<b>R 6.5</b> , 5.5, 6.32, 6.34
sch 1 HPP 11(4).....	<b>R 6.6</b> , 6.36
sch 1 HPP 11(6).....	5.5, 5.6, 5.15, 5.19, 5.50, 5.52
sch 1 HPP 12, 14.....	3.12, 3.14
sch 1 HPP 15.....	3.13, 3.14
sch 1 HPP 15(2)(a) .....	4.15, 4.19, 4.20
<i>Health Records and Information Privacy Code of Practice 2005</i> .....	3.15, 7.24
<i>Health Records and Information Privacy Regulation 2006</i> .....	2.3
<i>Interpretation Act 1987</i> .....	1.20, 11.12
s 13A.....	2.6
s 21(1) .....	11.8
s 33.....	1.20
s 41 .....	7.4
<i>Local Government Act 1993</i> .....	8.16
s 220(1) .....	11.8
<i>Medical Practice Act 1992</i>	
sch 1 cl 21-22.....	8.40
 <i>National Trust of Australia (New South Wales) Act 1990</i>	



s 4 .....	2.8
<i>Nature Conservation Trust Act 2001</i>	
s 9 .....	2.8
<i>Ombudsman Act 1974</i> .....	2.54, 4.36, 11.31
s 13A .....	9.20
s 13AA .....	<b>R 4.4</b> , 4.33, 4.35
s 20 .....	11.27
s 26 .....	9.18
s 35A .....	2.52, 2.54
s 35B .....	2.54
<i>Police Act 1990</i>	
pt 8A .....	<b>R 6.8</b> , 6.49, 6.54-6.55
s 122 .....	6.53, 6.55
s 140 .....	6.54
s 169A .....	6.52
<i>Privacy and Personal Information Protection Act 1998</i>	
pt 2, div 3 .....	4.1, 7.20, 7.49-7.50
pt 3 .....	7.15
pt 3, div 1 .....	4.1, 7.18
pt 4 .....	11.6
pt 4, div 3 .....	11.38, 11.40, 11.44
pt 5 .....	<b>R 12.1</b> , 7.23, 9.9, 9.12, 9.25, 12.9
pt 6 .....	7.5, 8.1, 8.3, 8.24, 8.36
s 3 .....	<b>R 5.1</b> , 2.1, 2.3, 2.37, 4.3, 5.3-5.4, 5.22, 5.44, 5.46, 7.4, 8.3, 10.33
s 4 .....	4.1, 4.4
s 4(3) .....	4.4
s 4(3)(a) .....	4.4
s 4(3)(b) .....	8.1, 8.4, 8.7
s 4(3)(g) .....	6.13

s 4(3)(h) .....	6.49, 6.51
s 4(3)(j).....	6.44
s 4(3)(k).....	4.4
s 4(4) .....	2.39
s 4A.....	4.1
s 5.....	5.41
s 6.....	<b>R 6.1-6.2</b> , 2.30, 4.1, 6.2, 6.4, 6.13
s 6(3).....	6.3
s 8.....	<b>R 6.7</b> , 6.42-6.43
s 9.....	3.4, 3.42, 3.59, 3.76, 3.78, 4.15, 4.20, 5.3-5.4, 5.17, .....5.26, 5.53, 6.19, 6.27, 7.47, 7.79
s 9(a).....	3.38
s 10.....	3.8, 4.15, 4.20, 5.3-5.4, 5.17, 5.26, 5.53, 6.19, 6.22, .....6.26-6.29, 7.40, 7.79
s 11.....	7.79
s 11(3) .....	6.34
s 12.....	2.45
s 12(a) .....	5.4, 5.31
s 12(c).....	6.16
s 13 .....	4.15, 4.20, 5.17, 5.41
s 14 .....	3.78, 4.15, 4.20, 5.17, 5.41
s 15.....	4.15, 4.20, 5.17, 5.41
s 16.....	4.35
s 17.....	<b>R 6.7</b> , 3.6, 4.15, 4.20, 4.35, 5.3-5.4, 5.7, 5.17, 6.36, .....6.42-6.43, 7.45, 7.79
s 18.....	<b>R 6.7</b> , 3.5, 3.8, 4.15, 4.20, 4.34-4.35, 5.3-5.4, 5.7, 5.17, .....5.51, 6.19, 6.24-6.25, 6.29, 6.36, 6.42-6.43, 7.45, 7.56, 7.79
s 19.....	3.7-3.8, 4.15, 4.20, 5.3, 5.17, 5.20, 6.19, 6.24, 6.29, 6.32, 6.36
s 19(1) .....	<b>R 6.7</b> , 4.35, 5.17, 5.20, 5.51, 6.33, 6.35, 6.42-6.43
s 20(1) .....	4.5

s 20(5) .....4.1, 5.41

s 23 .....**R 5.1**-5.2, 5.3, 5.5, 5.7, 5.20, 5.21, 5.24, 5.35, 5.41, 5.43-5.45

s 23(1) .....5.25

s 23(2) .....5.25

s 23(3) .....5.30

s 23(4), (5) .....5.7, 5.33

s 23(7) .....5.20, 5.33

s 24 .....**R 5.1**, 5.3, 5.4, 5.8, 5.13, 5.20-5.21, 5.24, 5.41, 5.43, 5.52, 7.51

s 24(1) .....5.25, 5.30, 5.53

s 24(2) .....5.33, 5.51

s 24(3) .....5.33, 5.51

s 24(4) .....5.18, 5.33, 5.51, 7.51

s 24(6) ..... 5.25-5.26, 5.53

s 24(7) .....5.31

s 25 ..... **R 4.1**, 4.14-4.25, 4.29, 4.35-4.36 5.23, 5.41, 5.52

s 25(a) .....**R 4.2-4.3**, 4.18, 4.21

s 25(b) .....**R 4.2**, 4.18, 4.22, 4.24, 4.32-4.33

s 26 ..... **R 6.3**, 6.18, 6.27, 6.30

s 26(1) .....**R 6.4**, 6.19, 6.21-6.23, 6.27, 6.31

s 26(2) .....3.4, 3.8, 6.19, 6.24-6.26, 6.29, 6.31

s 27 ..... **R 5.4-5.5**, 5.54-5.68

s 28(1) .....**R 6.5**, 6.32-6.35

s 28(3) .....**R 6.6**, 6.36-6.37

s 29(1) .....7.18

s 29(2) .....7.18, 7.35, 7.36

s 29(3)-(5) .....7.19

s 29(6)-(7) .....7.20

s 29(7)(b) .....7.31

s 30(1) .....7.18, 7.35

s 30(2) .....	7.20
s 31 .....	7.22, 10.28
s 32 .....	7.23
s 33 .....	<b>R 10.5</b> , 7.5, 10.9
s 35 .....	10.6
s 36 .....	10.3, 10.15, 11.11, 11.33
s 36(2)(a) .....	10.3, 10.9
s 36(2)(b) .....	10.3, 10.28
s 36(2)(c) .....	10.3, 10.28
s 36(2)(e) .....	<b>R 10.3</b> , 10.3, 10.9
s 36(2)(f) .....	10.3, 10.8
s 36(2)(g) .....	10.3, 10.9
s 36(2)(h) .....	10.3, 10.28
s 36(2)(i) .....	10.3, 10.8
s 36(2)(j) .....	10.3, 10.28
s 36(2)(k) .....	<b>R 10.6</b> , 9.5, 10.3, 10.14-10.16, 11.3
s 36(2)(l) .....	10.3, 10.21, 11.3
s 37 .....	<b>R 11.1</b> , 11.3, 11.6-11.12, 11.15, 11.17, 11.25
s 38 .....	11.6-11.12, 11.15-11.16
s 38(1)-(2) .....	11.3
s 38(2)(a) .....	10.5
s 38(4) .....	11.5, 11.7, 11.12, 11.14-11.17, 11.24-11.25
s 39 .....	11.4
s 40 .....	10.9
s 40(3) .....	11.3
s 41 .....	<b>R 7.10-7.12</b> , 4.1, 5.12, 5.43, 7.36, 7.66, 7.84, 7.87
s 41(1) .....	7.66
s 41(2) .....	7.76
s 41(3) .....	7.66

s 42 ..... 11.3

s 43 ..... **R 11.1**, 11.5, 11.26

s 44 ..... 7.4, 10.6

s 45 ..... 7.23, 9.5, 10.14, 10.30-10.33, 11.1, 11.29, 11.37, 11.49

s 45(1) ..... **R 10.6**, **R 11.4**, 10.15-10.16, 11.28, 11.30, 11.33-11.34,  
 ..... 11.36, 11.41

s 45(2) ..... 11.37

s 45(3)-(4) ..... 11.28

s 45(5) ..... 11.28, 11.41

s 45(6) ..... 11.41

s 46 ..... 10.31

s 46(1) ..... 11.38

s 46(2) ..... 11.37-11.38, 11.42

s 46(3) ..... 11.38, 11.41

s 46(6) ..... 11.38

s 47 ..... 9.12, 11.40-11.41

s 48 ..... 11.42

s 49 ..... **R 11.9**, 10.14, 11.44

s 49(3) ..... 9.45

s 50 ..... **R 11.9-11.11**, 10.14, 10.30-10.31, 10.33, 11.46, 11.48

s 51 ..... 11.43

s 52 ..... 9.4, 12.2-12.3

s 52(1)-(2) ..... 12.9

s 52(4) ..... 12.21

s 53 ..... 9.4, 12.3, 12.21, 12.25

s 53(1) ..... 12.8

s 53(2) ..... 12.3

s 53(3) ..... **R 12.3**, 12.14

s 53(3)(d) ..... 12.13

s 53(3)(e) ..... 7.4

s 53(4)-(5) .....	12.4
s 53(6) .....	12.5
s 53(7) .....	9.44, 12.6
s 53(7A) .....	12.6
s 53(8) .....	<b>R 12.5</b> , 12.7, 12.21
s 54 .....	10.9
s 54(1)-(2) .....	12.11
s 54(3)-(4) .....	12.12
s 54(5) .....	12.3, 12.12
s 55 .....	9.4, 12.5, 12.19-12.20, 12.23
s 55(1) .....	12.18, 12.21
s 55(2) .....	<b>R 12.9</b> , 9.4, 9.44, 12.21, 12.27, 12.30
s 55(2)(g) .....	12.28
s 55(3) .....	12.21, 12.28
s 55(4) .....	12.27
s 55(4A) .....	12.27
s 55(5) .....	12.28
s 55(6) .....	10.14, 12.36, 12.38
s 55(7) .....	10.14, 12.36
s 56 .....	<b>R 12.11</b> , 9.4, 12.21, 12.37-12.38
s 57 .....	<b>R 8.5</b> , 8.9-8.10, 8.25, 8.45
s 58 .....	8.11, 8.19, 8.24
s 59 .....	<b>R 8.4</b> , R 8.6, 8.12-8.13, 8.24, 8.42, 8.45
s 60 .....	10.33
s 60(4) .....	11.15
s 62 .....	<b>R 9.5</b> , 9.45-9.46, 9.49, 9.51-9.52, 9.57, 9.60-9.61
s 62(2) .....	9.62
s 63 .....	9.45-9.46, 9.49, 9.51, 9.60
s 64 .....	10.7, 10.34

s 65 .....	10.28, 10.31, 10.33, 11.49
s 66, 66A .....	10.35
s 67 .....	9.45, 10.35, 11.24
s 68 .....	9.45, 10.35-10.36
s 71 .....	7.4, 8.32
Privacy and Personal Information Protection Bill 1998 .....	7.20
<i>Privacy and Personal Information Protection</i>	
<i>Regulation 2005</i> .....	2.3, 2.37, 7.5, 8.10, 8.16
<i>Privacy Code of Practice (General) 2003</i> .....	7.41, 7.58
pt 3 .....	8.10
pt 4 .....	7.48
cl 10 .....	7.43
cl 10(2) .....	3.15
cl 14(1)(d) .....	7.40
<i>Privacy Committee Act 1975</i>	
s 16 .....	11.9, 11.16
<i>Public Finance and Audit Act 1983</i> .....	2.3, 2.7-2.8, 2.25, 2.29, 2.34
s 4 .....	2.7
s 45F(1) .....	2.9
sch 2 .....	2.7, 2.25
<i>Public Sector Employment and Management Act 2002</i>	
s 165 .....	2.3
sch 4 .....	2.3
<i>Public Sector Management Act 1988</i> .....	2.3, 2.52
sch 1 .....	2.52
sch 3 .....	2.3
<i>Real Property Act 1900</i> .....	8.25
<i>Royal Commissions Act 1923</i> .....	2.29, 6.11

s 8 .....	6.12
s 12 .....	6.16
s 12A .....	6.12
s 18A .....	6.12
<i>Special Commissions of Inquiry Act 1983</i> .....	6.11
<i>State Owned Corporations Act 1989</i> .....	2.17, 2.19
s 20E .....	2.20
sch 5 .....	2.17, 2.19
<i>State Records Act 1998</i> .....	2.22, 7.5, 7.19
<i>Subordinate Legislation Act 1989</i> .....	7.90
s 3 .....	7.4
s 5 .....	7.13
<i>Workplace Surveillance Act 2005</i>	
s 26 .....	4.30
s 41 .....	4.30

## Northern Territory

### *Information Act 2002*

s 3 .....	1.21
sch 2 IPP 1.4 .....	7.46

## Queensland

<i>Information Privacy Act 2009</i> .....	2.42, 11.19
s 21(1)(a) .....	2.12
s 35, s 36 .....	2.42
s 113 .....	11.19
s 116 .....	11.13
s 119(2) .....	11.19
s 120 .....	11.20, 11.24
s 157 .....	7.30



s 188 .....	11.20
<i>Statutory Instruments Act 1992</i>	
s 49-51 .....	7.30
<b>Tasmania</b>	
<i>Government Business Enterprises Act 1995</i> .....	2.21
<i>Ombudsman Act 1978</i> .....	11.19
s 24(2)-(3) .....	11.21
<i>Personal Information Protection Act 2004</i> .....	11.19
s 3 .....	2.21
s 21(1) .....	11.21
sch 1 PIPP 1.4 .....	7.46
<b>Victoria</b>	
<i>Health Records Act 2001</i>	
s 6 .....	1.21
<i>Information Privacy Act 2000</i> ..... 1.22, 1.23, 2.21, 2.43, 3.36, 5.60, 5.66, 6.37, 7.28	
pt 4 .....	7.15
s 1 .....	1.21-1.22
s 1(c).....	1.24
s 3 .....	2.21, 3.36, 5.22, 5.44, 8.3, 8.8
s 3(b) .....	8.4
s 5 .....	1.21
s 5(a) .....	1.23
s 9(1)(a).....	6.37
s 9(1)(c).....	2.21
s 9(1)(e) .....	2.12
s 9(1)(f) .....	2.12
s 13 .....	5.60

s 16(4) .....	8.18, 8.31, 8.43, 8.45
s 17 .....	2.43
s 18 .....	7.28
s 19(4) .....	7.29
s 44(5) .....	10.21
s 45 .....	11.13
s 48 .....	10.21
s 58(i) .....	10.21
s 58(j) .....	10.13
s 64 .....	3.54
sch 1 IPP 1.4 .....	7.46
sch 1 IPP 2 .....	5.60
sch 1 IPP 2.1(f) .....	4.18
sch 1 IPP 6 .....	5.60
 <i>Public Administration Act 2004</i>	
s 5 .....	2.21
 <b>Western Australia</b>	
Information Privacy Bill 2007 .....	1.21
 <b>New Zealand</b>	
<i>Privacy Act 1993</i> .....	8.21-8.22, 8.38
pt 6 .....	7.15
s 59, s 60(1) .....	8.21