

NSW LAW REFORM COMMISSION

Report 123

Privacy principles

August 2009

© New South Wales Law Reform Commission, Sydney, 2009

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 978-0-7347-2638-4 (pbk)

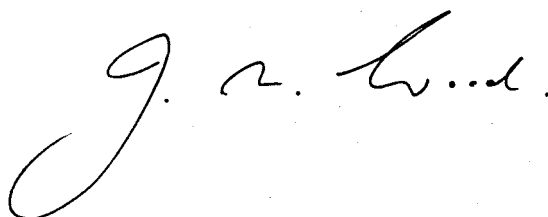
Letter to the Attorney General

To the Hon John Hatzistergos
Attorney General for New South Wales

Dear Attorney

Privacy principles

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

A handwritten signature in black ink, appearing to read "J. R. Wood". The signature is written in a cursive style with a large initial 'J' and a period after 'R'.

The Hon James Wood AO QC

Chairperson

August 2009

Table of Contents

Terms of Reference	x
Participants	xi
Abbreviations used in this report	xii
List of recommendations	xiii
MODEL UNIFIED PRIVACY PRINCIPLES (UPPs).....	xix
Introduction	1
BACKGROUND TO THIS REPORT	2
WHAT ARE PRIVACY PRINCIPLES?	3
ALRC'S APPROACH TO REVIEW OF PRIVACY.....	4
National uniformity	4
Application to public sector/private sector	6
Exemptions	6
PURPOSE OF THIS REPORT.....	7
Particular limitations	9
1. UPP1: Anonymity and pseudonymity	13
INTRODUCTION.....	14
What do anonymity and pseudonymity mean?	14
Limitations	15
Anonymity as a starting point	16
Precedents	17
Technologies: threat and opportunities	17
THE ALRC'S RECOMMENDATION	19
The current Commonwealth law.....	19
Extension of the anonymity principle to agencies	19
Pseudonymity.....	20
Content and application	22
THE CURRENT LAW IN NSW.....	27
SUBMISSIONS	27
THE COMMISSION'S CONCLUSIONS	28
2. UPP 2: Collection	31
INTRODUCTION.....	32
PURPOSES OF COLLECTION	33
The ALRC's recommendation	33
The current law in NSW	34
The Commission's conclusions.....	35
MEANS AND MANNER OF COLLECTION	37
COLLECTION FROM THE INDIVIDUAL CONCERNED	38
The ALRC's recommendations	38
The current law in NSW	40
Submissions.....	41
The Commission's conclusions.....	42
UNSOLICITED PERSONAL INFORMATION.....	44
The ALRC's recommendations	45

The law in NSW	47
Submissions	51
The Commission's conclusions	52
SENSITIVE INFORMATION	53
Current law	54
Regulating the collection of sensitive information	56
3. UPP 3: Notification.....	71
INTRODUCTION.....	72
A SEPARATE PRINCIPLE.....	73
NATURE AND TIMING	74
Notification as a means of ensuring awareness.....	74
Timing	76
Reasonable steps include no steps.....	77
EXEMPTIONS.....	79
The law in NSW	81
The Commission's conclusion.....	82
COLLECTION OF PERSONAL INFORMATION FROM A THIRD PARTY	84
The law in NSW	85
Submissions.....	86
The Commission's conclusion.....	87
CONTENT OF NOTIFICATION.....	87
The fact and circumstances of collection	88
Collector's identity, individual's rights, and consequences of not providing information.....	90
Purposes for which information is collected	92
Entities to which information is usually disclosed.....	94
Avenues of complaint.....	95
Information required or authorised by or under law.....	97
4. UPP 4: Openness.....	99
ALRC REPORT 108.....	100
Model Unified Privacy Principle 4.....	100
The rationale behind Recommendation 24-1	102
NSWLRC'S CONSULTATION PAPER 3	107
CONCLUSION	108
5. UPP 5: Use and disclosure	111
INTRODUCTION.....	112
Use	112
Disclosure	113
ALRC REPORT 108.....	114
Model Unified Privacy Principle 5.....	114
How does UPP 5 differ from the current Commonwealth principles?.....	117
What is the rationale behind UPP 5?	120
CONSULTATION PAPER 3	126
One principle.....	126

Form of the principle	127
THE COMMISSION'S CONCLUSIONS	133
One principle	133
Form of the principle	135
6. UPP 6: Direct marketing	143
WHAT IS "DIRECT MARKETING"?	144
RELEVANCE FOR NSW	144
ALRC REPORT 108	145
Rationale for excluding agencies from the ambit of the direct marketing principle	145
A direct marketing principle to apply to organisations	147
How does UPP 6 differ from the current Commonwealth principles?	149
THE COMMISSION'S VIEW	155
7. UPP 7: Data quality	157
ALRC REPORT 108	158
Model Unified Privacy Principle 7	158
The rationale behind Recommendation 27-1	159
PRIVACY LEGISLATION IN NSW: CONSULTATION PAPER 3	167
Current data quality provisions	167
Differences between the NSW provisions and UPP 7	168
Information collected indirectly from third parties	169
Unsolicited information	171
THE COMMISSION'S CONCLUSIONS	171
Should NSW adopt UPP 7?	171
Should there be a separate data quality principle regulating health information?	172
8. UPP 8: Data security	173
INTRODUCTION	174
WHAT IS A DATA SECURITY BREACH?	174
ALRC RECOMMENDATION	175
Model Unified Principle 8	175
FORMULATION OF UPP 8	175
Current data security obligations	175
A single principle	177
Reference to data breach notification provisions	178
Prevention of loss and misuse	180
Destruction and retention of personal information	185
PRIVACY LEGISLATION IN NSW	190
Current data security provisions	190
NSWLRC Consultation Paper 3	191
THE COMMISSION'S CONCLUSIONS	198

9. UPP 9: Access and correction	201
INTRODUCTION.....	202
NSWLRC CONSULTATION PAPER 3	205
ALRC DISCUSSION PAPER 72	208
ALRC REPORT 108.....	209
ACCESS	212
UPP 9.....	212
Current Commonwealth law	214
How and why is UPP 9 different from current Commonwealth law relating to the access of personal information?.....	214
Exemptions for agencies.....	215
Exemptions for organisations.....	216
Commercially sensitive information.....	218
Intermediaries	218
Procedural Requirements	220
Current law in NSW.....	224
How does NSW law differ from UPP 9?.....	226
CORRECTION	230
UPP 9.....	230
Current Commonwealth law	231
How and why is UPP 9 different from current Commonwealth law relating to the correction of personal information?.....	233
Current NSW law	244
NSWLRC Consultation Paper 3	245
How is NSW law different from the proposed UPP 9?	246
REFUSAL OF REQUEST TO ACCESS OR CORRECT.....	248
UPP 9.....	248
How UPP 9.8 is different from current Commonwealth law.....	249
How UPP 9.8 is different from NSW law	251
CONCLUSION	251
10. UPP 10: Identifiers	253
INTRODUCTION.....	254
Current legislative regulation of identifiers	254
Focus of this chapter.....	256
ALRC REPORT 108.....	256
Rationale for a separate identifier principle	257
Rationale for excluding government agencies	258
The proposed identifier principle	259
Ambit and distinguishing features of UPP 10	261
Practical application of UPP 10	269
Multi-purpose identifiers	271
THE COMMISSION'S VIEW	272

11. UPP 11: Cross-border data flows	273
INTRODUCTION.....	274
CURRENT APPROACHES TO REGULATION OF CROSS-BORDER	
DATA FLOWS.....	275
The adequacy approach	275
The accountability approach	277
The Australian approach	278
ALRC REPORT 108.....	282
CONTENT AND DISTINGUISHING FEATURES OF UPP 11	282
Coverage.....	282
Terminology	283
“Transfer”	283
Approach.....	285
DEFINING ACCOUNTABILITY	286
THE SCOPE OF APPLICATION OF UPP 11.....	288
Reasonable belief	288
Consent.....	293
“Required or authorised by or under law”	295
ADEQUACY OF REMEDIAL ACTION	297
INTERACTION WITH OTHER UPPs	298
THE COMMISSION’S OVERALL VIEWS	299
Appendix	301
Appendix A: Submissions.....	302

TERMS OF REFERENCE

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

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

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

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

PARTICIPANTS

Division members

His Honour Judge Kevin O'Connor AM

Professor Michael Tilbury (Commissioner-in-charge)

The Hon James Wood AO QC

Officers of the Commission

Executive Director

Ms Deborah Sharp (Acting)

Legal research and writing

Ms Lynsey Blayden

Ms Francesca Di Benedetto

Ms Catherine Gray

Mr Ani Luzung

Ms Sharminie Niles

Ms Abi Paramaguru

Librarian

Ms Anna Williams

Desktop publishing

Mr Terence Stewart

Administrative assistance

Ms Wendy Stokoe

ABBREVIATIONS USED IN THIS REPORT

In order to enhance the readability of the paper, abbreviations are employed for frequently repeated names and legislation. Rather than redefine these same abbreviations in each chapter, we have set them out below.

Agency/agencies	Public sector agency/agencies
ALRC	Australian Law Reform Commission
CP 3	New South Wales Law Reform Commission, <i>Privacy Legislation in New South Wales</i> (Consultation Paper 3, 2008)
DP 72	Australian Law Reform Commission, <i>Review of Australian Privacy Law</i> (Discussion Paper 72, 2007).
HRIPA	<i>Health Records and Information Privacy Act 2002</i> (NSW)
HPPs	NSW Health Privacy Principles
IPPs	NSW Information Protection Principles
NPPs	Commonwealth National Privacy Principles
NSWLRC	New South Wales Law Reform Commission
Organisation/s	Private sector organisation/s
Principles	Commonwealth Information Privacy Principles
Privacy Act	<i>Privacy Act 1988</i> (Cth)
PPIPA	<i>Privacy and Personal Information Protection Act 1998</i> (NSW)
Report 108	Australian Law Reform Commission, <i>For Your Information: Australian Privacy Law and Practice</i> (Report 108, 2008)
UPPs	Unified Privacy Principles

LIST OF RECOMMENDATIONS

RECOMMENDATION 1 - *see page 37*

UPP 2.1 should be modified as follows:

2.1 An agency or organisation must not collect personal information unless it is *reasonably* necessary for one or more of its functions or activities.

RECOMMENDATION 2 - *see page 37*

The 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.

RECOMMENDATION 3 - *see page 44*

UPP 2.3 should be revised to read as follows:

2.3 An agency or organisation may collect personal information otherwise than directly from the individual to whom the information relates when either:

- the individual has authorised the collection of the information from someone else; or
- collection from the individual is not reasonable or practicable under the circumstances.

RECOMMENDATION 4 - *see page 92*

UPP 3(e) should be modified in the following way:

UPP 3. Notification

At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of, the:

...

(e) main consequences (*if any*) of not providing *all or part of* the information.

RECOMMENDATION 5 - *see page 137*

UPP 5.1(a) should be modified in the following way:

5.1 An agency must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection (the secondary purpose) unless:

(a) both of the following apply:

- (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 to use or disclose the information for the secondary purpose *and the agency has no reason to believe that the individual would object.*

RECOMMENDATION 6 - *see page 139*

UPP 5.1(d) should be modified in the following way:

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.

RECOMMENDATION 7 - *see page 140*

"Primary purpose" in UPP 5 should be defined to mean the purpose for which the agency or organisation collected the personal information.

RECOMMENDATION 8 - *see page 142*

"Sensitive information" should be defined to mean:

- (a) information or an opinion about an individual's:
 - (i) racial or ethnic origin; or
 - (ii) political opinions; or
 - (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association, or a trade union; or
 - (vii) sexual preferences or practices; or
 - (viii) *criminal history, including criminal record*, that is also personal information; or
- (b) health information about an individual; or
- (c) genetic information about an individual that is not otherwise health information.

RECOMMENDATION 9 - *see page 194*

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that the privacy principles apply to personal information held, or collected for inclusion, in a record or generally available publication.

RECOMMENDATION 10 - *see page 198*

UPP 8 should be amended as follows:

UPP 8. Data Security

8.1 An agency or organisation must take reasonable steps to:

- (a) ...
- (b) ...
- (c) *ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.*

RECOMMENDATION 11 - *see page 198*

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 a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an Information Privacy Principle if done or engaged in by the agency; and
- (2) to ensure that the contract does not authorise a contracted service provider for the contract to do or engage in such an act or practice.

RECOMMENDATION 12 - *see page 272*

UPP 10.4 should be amended so as to remove the exclusion of ABNs from the definition of identifiers.

RECOMMENDATION 13 - *see page 288*

An agency or organisation being “accountable” for personal information should be defined in UPP 11 to mean:

- (a) being responsible for the acts and practices of a recipient of personal information, the subject of a cross-border transfer; and
- (b) being liable for a breach of UPP 11 if the acts and practices of the recipient would have amounted to an interference with the privacy of an individual, if done in Australia.

RECOMMENDATION 14 - *see page 292*

If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient who is outside of Australia and an external territory, the agency or organisation should remain accountable for that personal information unless the recipient of the information is subject to a law that effectively upholds privacy protections that are substantially similar to, or more favourable than, the protections afforded by privacy legislation in Australia and that applies in a “listed jurisdiction”. A “listed jurisdiction” is one that is specifically identified in a legislative instrument for the purposes of UPP 11.

RECOMMENDATION 15 - *see page 292*

In UPP 11 binding schemes should be dealt with in the same way as laws.

RECOMMENDATION 16 - *see page 293*

The “reasonable belief” test in relation to contracts should be replaced with a test that requires the contract to contain mandatory terms which incorporate privacy protections that are substantially similar to, or more favourable than, the protections afforded by privacy legislation in Australia.

RECOMMENDATION 17 - *see page 295*

UPP 11.1(b) should be amended to read as follows:

(b) the individual expressly consents to the transfer, after being expressly notified of the following:

- (i) the destination jurisdiction/s of the transfer and the likelihood of further transfers;
- (ii) the intended recipient/s;
- (iii) the intended uses (if known);and
- (iv) the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred.

RECOMMENDATION 18 - *see page 298*

Note 3 to UPP 5 should be deleted and the Note to UPP 11 should be replaced with a note stating that agencies and organisations are subject to the requirements of all other principles when transferring personal information about an individual to a recipient who is outside Australia.

MODEL UNIFIED PRIVACY PRINCIPLES (UPPs)

The Model Unified Privacy Principles (UPPs) are those developed by the Australian Law Reform Commission. They are reproduced from its report *For Your Information: Australian Privacy Law and Practice* Report 108 (2008) vol 1, 91-102. Modifications recommended to the UPPs in this report are set out in bold or are struck through.

The UPPs should be read in conjunction with the following:

- *The Commission recommends that the privacy legislation 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.*
- *The Commission also recommends that “sensitive information” be defined to mean:*
 - (a) *information or an opinion about an individual’s:*
 - (i) *racial or ethnic origin; or*
 - (ii) *political opinions; or*
 - (iii) *membership of a political association; or*
 - (iv) *religious beliefs or affiliations; or*
 - (v) *philosophical beliefs; or*
 - (vi) *membership of a professional or trade association, or a trade union; or*
 - (vii) *sexual preferences or practices; or*
 - (viii) *criminal history, including criminal record that is also personal information; or*
 - (b) *health information about an individual; or*
 - (c) *genetic information about an individual that is not otherwise health information.*

UPP 1 Anonymity and Pseudonymity

Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:

- (a) not identifying themselves; or
- (b) identifying themselves with a pseudonym.

UPP 2 Collection

2.1 An agency or organisation must not collect personal information unless it is **reasonably** necessary for one or more of its functions or activities.

2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

2.3 An agency or organisation may collect personal information otherwise than directly from the individual to whom the information relates when either:

- (a) the individual has authorised the collection of the information from someone else; or**
- (b) collection from the individual is not reasonable or practicable under the circumstances.**

2.4 If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either:

- (a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or
- (b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had actively collected the information.

2.5 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:

- (a) the individual has consented;

- (b) the collection is required or authorised by or under law;
- (c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information concerns is legally or physically incapable of giving or communicating consent;
- (d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual to whom the information concerns that the organisation will not disclose the information without the individual's consent;
- (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;
- (f) the collection is necessary for research and all of the following conditions are met:
 - (i) the purpose cannot be served by the collection of information that does not identify the individual or from which the individual would not be reasonably identifiable;
 - (ii) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection;
 - (iii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*; and

- (iv) the information is collected in accordance with Research Rules issued by the Privacy Commissioner; or
- (g) the collection is necessary for the purpose of a confidential alternative dispute resolution process.

2.6 Where an agency or organisation collects sensitive information about an individual in accordance with 2.5(f), it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Note: Agencies and organisations that collect personal information about an individual from an individual or from someone else must comply with UPP 3.

UPP 3 Notification

3. At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of, the:

- (a) fact and circumstances of collection, where the individual may not be aware that his or her personal information has been collected;
- (b) identity and contact details of the agency or organisation;
- (c) rights of access to, and correction of, personal information provided by these principles;
- (d) purposes for which the information is collected;
- (e) main consequences (**if any**) of not providing **all or part of** the information.
- (f) actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information of the kind collected;
- (g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of

his or her personal information are set out in the agency's or organisation's Privacy Policy; and

- (h) fact, where applicable, that the collection is required or authorised by or under law.

UPP 4 Openness

4.1 An agency or organisation must create a Privacy Policy that sets out clearly its expressed policies on the management of personal information, including how it collects, holds, uses and discloses personal information. This document should also outline the:

- (a) sort of personal information the agency or organisation holds;
- (b) purposes for which personal information is held;
- (c) avenues of complaint available to individuals in the event that they have a privacy complaint;
- (d) steps individuals may take to gain access to personal information about them held by the agency or organisation; and
- (e) whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.

4.2 An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual:

- (a) electronically; and
- (b) on request, in hard copy, or in an alternative form accessible to individuals with special needs.

UPP 5 Use and Disclosure

5.1 An 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:

- (a) both of the following apply:
 - (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;**
- (b) the individual has consented to the use or disclosure;
- (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;
- (d) 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;
- (e) the use or disclosure is required or authorised by or under law;
- (f) 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;
- (g) the use or disclosure is necessary for research and all of the following conditions are met:
 - (i) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the use or disclosure;
 - (ii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act;
 - (iii) the information is used or disclosed in accordance with Research Rules issued by the Privacy Commissioner; and
 - (iv) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the information in a form that would identify the individual or from which the individual would be reasonably identifiable; or
- (h) the use or disclosure is necessary for the purpose of a confidential alternative dispute resolution process.

5.2 If an agency or organisation uses or discloses personal information under paragraph 5.1(f) it must make a written note of the use or disclosure.

5.3 UPP 5.1 operates in respect of personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

5.4 In UPP 5 “primary purpose” means the purpose for which the agency or organisation collected the personal information.

Note 1: It is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 5.1 does not override any existing obligations not to disclose personal information. 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.

~~Note 3: Agencies and organisations also are subject to the requirements of the 'Cross-border Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.~~

UPP 6 Direct Marketing (only applicable to organisations)

6.1 An organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing only where the:

- (a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and
- (b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications.

6.2 An organisation may use or disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing only in the following circumstances:

- (a) either the:
 - (i) individual has consented; or
 - (ii) information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure;
- (b) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays a notice advising the individual, that he or she may express a

wish not to receive any further direct marketing communications;

- (c) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and
- (d) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual's personal information.

6.3 In the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must:

- (a) comply with this requirement within a reasonable period of time; and
- (b) not charge the individual for giving effect to the request.

UPP 7 Data Quality

An agency or organisation must take reasonable steps to make certain that the personal information it collects, uses or discloses is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.

UPP 8 Data Security

8.1 An agency or organisation must take reasonable steps to:

- (a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure; and
- (b) 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 and retention is not required or authorised by or under law.
- (c) **ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is**

protected from being used or disclosed by that person otherwise than in accordance with the UPPs.

8.2 The requirement to destroy or render non-identifiable personal information is not 'required by law' for the purposes of the *Archives Act 1983* (Cth).

Note: Agencies and organisations also should be aware of their obligations under the data breach notification provisions.

UPP 9 Access and Correction

9.1 If an agency or organisation holds personal information about an individual and the individual requests access to the information, it must respond within a reasonable time and provide the individual with access to the information, except to the extent that:

Where the information is held by an agency:

- (a) the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; or

Where the information is held by an organisation:

- (b) providing access would be reasonably likely to pose a serious threat to the life or health of any individual;
- (c) providing access would have an unreasonable impact upon the privacy of individuals other than the individual requesting access;
- (d) the request for access is frivolous or vexatious;
- (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings;
- (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- (g) providing access would be unlawful;

- (h) denying access is required or authorised by or under law;
- (i) providing access would be likely to prejudice an investigation of possible unlawful activity;
- (j) providing access would be likely to prejudice the:
 - (i) 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) enforcement of laws relating to the confiscation of the proceeds of crime;
 - (iii) protection of the public revenue;
 - (iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (v) preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;
 by or on behalf of an enforcement body; or
- (k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

9.2 Where providing access would reveal evaluative information generated within the agency or organisation in connection with a commercially sensitive decision-making process, the agency or organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: The mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information under UPP 9.2.

9.3 If an agency or organisation is not required to provide an individual with access to his or her personal information it must take such steps, if any, as are reasonable to provide the individual with as much of the information as possible, including through the use of a mutually agreed intermediary.

9.4 If an organisation charges for providing access to personal information, those charges:

- (a) must not be excessive; and
- (b) must not apply to lodging a request for access.

Note: Agencies are not permitted to charge for providing access to personal information under UPP 9.4.

9.5 An agency or organisation must provide personal information in the manner requested by an individual, where reasonable and practicable.

9.6 If an agency or organisation holds personal information about an individual that is, with reference to a purpose for which it is held, misleading or not accurate, complete, up-to-date and relevant, the agency or organisation must take such steps, if any, as are reasonable to:

- (a) correct the information so that it is accurate, complete, up-to-date, relevant and not misleading; and
- (b) notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

9.7 If an individual and an agency or organisation disagree about whether personal information is, with reference to a purpose for which the information is held, misleading or not accurate, complete, up-to-date or relevant and:

- (a) the individual asks the agency or organisation to associate with the information a statement claiming that the information is misleading or not accurate, complete, up-to-date or relevant; and
- (b) where the information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the agency or organisation must take reasonable steps to do so.

9.8 Where an agency or organisation denies a request for access or refuses to correct personal information it must provide the individual with:

- (a) reasons for the denial of access or refusal to correct the information, except to the extent that providing such reasons would undermine a lawful reason for denying access or refusing to correct the information; and
- (b) notice of potential avenues for complaint.

UPP 10 Identifiers (only applicable to organisations)

10.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

- (a) an agency;
- (b) an agent of an agency acting in its capacity as agent;
- (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or
- (d) an Australian state or territory agency.

10.2 Where an identifier has been ‘assigned’ within the meaning of UPP 10.1 an organisation must not use or disclose the identifier unless:

- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency that assigned the identifier;
- (b) one or more of UPP 5.1(c) to (f) apply to the use or disclosure; or
- (c) the identifier is genetic information and the use or disclosure would be permitted by the new *Privacy (Health Information) Regulations*.

10.3 UPP 10.1 and 10.2 do not apply to the adoption, use or disclosure by a prescribed organisation of a prescribed identifier in prescribed circumstances, set out in regulations made after the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned.

10.4 The term ‘identifier’, for the purposes of UPP 10, includes a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:

- (a) uniquely identifies or verifies the identity of an individual for the purpose of an agency’s operations; or
- (b) is determined to be an identifier by the Privacy Commissioner.

~~However, an individual’s name or ABN, as defined in the A New Tax System (Australian Business Number) Act 1999 (Cth), is not an ‘identifier’.~~

Note: A determination referred to in the ‘Identifiers’ principle is a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act* 2003 (Cth).

UPP 11 Cross-border Data Flows

11.1 If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless:

- (a) the recipient of the information is subject to:**
 - (i) a law or binding scheme that effectively upholds privacy protections that are substantially similar to, or more favourable than, the protection afforded by privacy legislation in Australia and that applies in a listed jurisdiction; or**
 - (ii) a contract containing mandatory contract terms which incorporate privacy protections that are substantially similar to, or more favourable than, the protection afforded by privacy legislation in Australia;**
- (b) the individual expressly consents to the transfer, after being expressly notified of the following:**
 - (i) the destination jurisdiction/s of the transfer and the likelihood of further transfers;**
 - (ii) the intended recipient/s;**

(iii) the intended uses (if known); and

(iv) the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or

- (c) the agency or organisation is required by or under law to transfer the personal information.

An agency or organisation being “accountable” for personal information means:

- (a) being responsible for the acts and practices of a recipient of personal information, the subject of a cross-border transfer; and**
- (b) being liable for a breach of UPP 11 if the acts and practices of the recipient would have amounted to an interference with the privacy of an individual, if done in Australia.**

A “listed jurisdiction” is one that is specifically identified in a legislative instrument for the purposes of UPP 11.

Note Agencies and organisations are also subject to the requirements of all the other principles when transferring personal information about an individual to a recipient who is outside Australia.

Introduction

- Background to this report
- What are privacy principles?
- ALRC's approach to review of privacy
- Purpose of this report

BACKGROUND TO THIS REPORT

0.1 In terms of reference issued on 11 April 2006 by the then Attorney General, the Hon R J Debus MP, the Commission was asked to “inquire into and report on whether existing legislation in NSW provides an effective framework for the protection of the privacy of an individual”. In undertaking this review, the Commission was asked to consider, among other issues, the desirability of privacy protection principles being uniform across Australia. The Commission was specifically asked to liaise with the Australian Law Reform Commission (“ALRC”).

0.2 The Commission divided the work into stages and, in the first stage of the project, examined whether or not a statutory cause of action for breach of privacy should be introduced in NSW. A consultation paper was published in May 2007, which outlined a possible statutory cause of action and sought community response.¹ A final report, proposing a statutory cause of action for invasion of privacy as part of a uniform law reform exercise, was completed in April 2009.²

0.3 In the second phase, the Commission focused on the legislative approach to privacy within NSW. Consultation Paper 3, *Privacy Legislation in New South Wales* (“CP 3”), published in June 2008, evaluated the effectiveness of the key NSW statutes that protect privacy, namely: the *Privacy and Personal Information Protection Act 1998* (NSW); the *Health Records and Information Privacy Act 2002* (NSW); the *Freedom of Information Act 1989* (NSW); the *Local Government Act 1993* (NSW); and the *State Records Act 1998* (NSW). CP 3 analysed the privacy principles in depth and made numerous proposals for reform.³

0.4 For reasons that are explained below, in this next phase of the privacy reference, we have isolated review of the privacy principles before proceeding to report on the balance of the issues canvassed in CP 3.

-
1. NSW Law Reform Commission, *Invasion of Privacy* Consultation Paper 1 (2007).
 2. NSW Law Reform Commission, *Invasion of Privacy* Report 120 (2009).
 3. NSW Law Reform Commission, *Privacy Legislation in New South Wales* Consultation Paper No 3 (2008) (“NSWLRC CP 3”), Ch 3 and 6.

WHAT ARE PRIVACY PRINCIPLES?

0.5 Privacy principles regulate privacy by setting out general rules that “express the fundamental obligations that all should observe”.⁴ Principles do not:

necessarily prescribe detailed steps that must be complied with, but rather [set] an overall objective that must be achieved. In this way, principles-based regulation seeks to provide an overarching framework that guides and assists regulated entities to develop an appreciation of the core goals of the regulatory scheme.⁵

By being framed at a higher, more general level than detailed, prescriptive rules, principles allow for broad application and flexibility, both across jurisdictions and entities, and in changing situations and developing technological contexts.

0.6 Taking a principles-based approach to privacy regulation, as opposed to a rules-based approach, shifts the focus of the legislation from *process* to *outcomes*.⁶ In its Report 108, the ALRC quoted Professor Black to explain the rationale for this:

Regulators, instead of focussing on prescribing the processes or actions that firms must take, should step back and define the outcomes that they require firms to achieve. Firms and their management will then be free to find the most efficient way of achieving the outcome required.⁷

0.7 Current privacy legislation in both the Commonwealth and NSW takes a principles-based approach to the regulation of information privacy. The ALRC has indicated that this is its preferred approach in any amended Commonwealth legislation. Subject to two caveats, highlighted in the two following paragraphs, the Commission supports this view and favours a continued principles-based approach to information privacy regulation in NSW.

-
4. J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (London School of Economics and Political Science, 2007), 3.
 5. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) vol 1 [4.7].
 6. ALRC Report 108 vol 1 [4.6].
 7. J Black, *Principles Based Regulation: Risks, Challenges and Opportunities*, 5, quoted in ALRC Report 108 vol 1 [4.6].

0.8 A regime that is underpinned by high-level principles needs to be augmented by privacy guidelines and regulations, which is what the ALRC proposes. In theory, this is a sound scheme. However, in practice, privacy regulation will only remain effective if regulations clarify and strengthen, not dilute, the default standards set in privacy principles,⁸ and privacy guidelines are supported by effective enforcement.⁹

0.9 This is particularly relevant for NSW's health industry in light of the Commission's proposal, and the ALRC's recommendation, to hand over responsibility for regulating privacy in the private sector to the Commonwealth, discussed in detail below. The Commission questioned in CP 3 whether, if health information held by the private sector were regulated by the *Privacy Act 1988* (Cth), there would still be a need for the continued existence of the *Health Records and Information Privacy Act 2002* (NSW).¹⁰ It would be a matter for concern if the current high standards set for the protection of health information privacy by the *Health Records and Information Privacy Act 2002* (NSW) were weakened by regulations passed pursuant to the *Privacy Act 1988* (Cth). For this reason, the Commission urges that the default standards in the UPPs not be undermined by regulations.

ALRC'S APPROACH TO REVIEW OF PRIVACY

National uniformity

0.10 National uniformity is one of the key areas of focus of a concurrent inquiry into Australia's privacy laws by the ALRC. In September 2007, the ALRC published its Discussion Paper 72, *Review of Australian Privacy Law*,¹¹ and in May 2008 it published its final report, *For Your Information: Australian Privacy Law and Practice* ("Report 108"). The cornerstone of

8. See N Waters and G Greenleaf, "Meeting Privacy Challenges – the ALRC and NSWLRC Privacy Reviews", Paper given at Cyberspace Law and Policy Centre, University of New South Wales Symposium, Panel Session 3: "How do the ALRC and NSWLRC proposals contribute to providing a set of global best practice Privacy Principles which also adequately address the privacy threats and opportunities from emerging technologies?" 2 October 2008 ("Waters and Greenleaf") 6.

9. Waters and Greenleaf, 6.

10. NSWLRC CP 3 Issue 4.

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

Report 108 is the premise that privacy laws should be consistent across all Australian jurisdictions.¹²

0.11 The Commission’s CP 3 likewise emphasised the desirability of a consistent legislative approach to privacy both nationally and within NSW itself. It proposed that reforms of NSW privacy law should aim to achieve national uniformity¹³ and that NSW should co-operate with the Commonwealth in the development of privacy principles that are capable of application in all NSW privacy legislation.¹⁴

0.12 In pursuit of uniformity, the ALRC has recommended the development of Unified Privacy Principles (“UPPs”) and the enactment by the States and Territories of legislation that applies these and adopts relevant definitions used in the *Privacy Act 1988* (Cth).¹⁵ The ALRC has formulated 11 UPPs, which it recommends serve as the framework of national consistency. These are set out below and each is discussed in the chapters that follow this Introduction:

- UPP 1 – Anonymity and Pseudonymity
- UPP 2 – Collection
- UPP 3 – Notification
- UPP 4 – Openness
- UPP 5 – Use and Disclosure
- UPP 6 – Direct Marketing
- UPP 7 – Data Quality
- UPP 8 – Data Security
- UPP 9 – Access and Correction
- UPP 10 – Identifiers
- UPP 11 – Cross-border Data Flows

0.13 The UPPs are drafted at a high level of generality to allow for flexibility in their application to different jurisdictions. As explained above, the Commission supports this approach, noting in CP 3 that high-level principles accommodate the differences in practices and obligations

12. ALRC Report 108 vol 1 [3.13]-[3.15] Recommendation 3-4.

13. NSWLRC CP 3 Proposal 1.

14. NSWLRC CP 3 Proposal 2.

15. ALRC Report 108 vol 1 [3.13]-[3.15] Recommendation 3-4.

across jurisdictions, public and private sectors, and individual businesses. High-level privacy principles are also capable of accommodating the particularity of health information.

Application to public sector/private sector

0.14 Under the *Privacy Act 1988* (Cth), public sector agencies and private sector organisations are regulated by separate sets of privacy principles. Agencies are regulated by 11 Information Privacy Principles, set out in s 14 of the Act, and organisations are regulated by 10 National Privacy Principles set out in Schedule 3 to the Act. They are quite different from each other. The UPPs represent a major departure from this model in that, except for UPPs 6 and 10,¹⁶ they apply to both agencies and organisations.¹⁷ This feature should be kept in mind in approaching the discussion of each of the UPPs.

Exemptions

0.15 Report 108 devotes an entire part, Part E, to exemptions. This part includes a discussion of: exemptions from the Privacy Act; exemptions for specified bodies, such as intelligence and defence intelligence agencies, federal courts and tribunals, agencies with law enforcement functions, and exempt agencies under the *Freedom of Information Act 1982* (Cth); other public sector exemptions; the exemption for small business; the employee records exemption; a political exemption; a journalism exemption; other private sector exemptions; and a recommended new partial exception for alternative dispute resolution.¹⁸

0.16 The Cyberspace Law and Policy Centre note that the ALRC recommends “removal of many of the existing exemptions, such as those for employee records, small business and political parties, acts and practices, and narrowing of the media exemption, and review of many of the arbitrary 'inherited' exemptions for specific government agencies”. The Centre points out that, “these recommendations would mean a major extension of the coverage of the privacy principles, with privacy

16. These UPPs only apply to organisations.

17. Although, within UPP 9 there are slight differences in application depending on whether the information is held by an agency or organisation. Also, UPP 2 contains a sub-section, UPP 2.5(d) that applies only to non-profit organisations.

18. ALRC Report 108 vol 2 Recommendation 44-1.

obligations and rights applying in many circumstances where they are most necessary”.¹⁹

0.17 Similarly, in CP 3, the Commission canvassed the exemptions under the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW), including exceptions to what constitutes “personal information”, and proposed changes to eliminate or limit many exceptions, thereby expanding the scope of those Acts and the application of the Information Protection Principles and Health Privacy Principles.²⁰

0.18 Clearly, the number and form of exemptions has a direct bearing on the application of the UPPs. However, this is more from the perspective of the breadth of their ambit, rather than the content of each. As indicated above, it is the Commission’s intention to focus on the broader question of exemptions in the next phase of this reference, once again, in this report, distilling the issues strictly pertaining to the UPPs themselves. Hence, where there are exemptions contained within a particular UPP, and relevant in the specific context of that UPP, these are analysed in the dedicated chapter. What this report does not deal with is general exemptions from all or parts of the Commonwealth and NSW privacy Acts.

PURPOSE OF THIS REPORT

0.19 This paper constitutes a step in the continuum of reform of privacy law within NSW, making recommendations that are directed to NSW but intended to apply uniformly. The purpose of this paper is to evaluate the UPPs for their feasibility and efficacy as principles to be incorporated into NSW’s privacy legislation. The objective of achieving national uniformity dictates that the UPPs should be both capable of incorporation into State and Territory legislation, and acceptable to the States and Territories in terms of the value and effectiveness of the UPPs: the States and Territories must be both willing and able to adopt the UPPs.

0.20 We have chosen to keep the focus of this paper concentrated. We are mindful that there are many intertwined issues that require resolution, including the interaction of privacy laws with other legislation, especially freedom of information legislation, and questions

19. Waters and Greenleaf, 2.

20. NSWLRC CP 3 Ch 5 and 7.

as basic as what “personal information” should encompass, and, therefore, to what personal information the UPPs should apply. By keeping this report so narrowly focused, the Commission in no way intends to ignore those issues or underestimate their significance and complexity. We have taken the view that it is important to get the UPPs right, first and foremost, as they will underpin State and Commonwealth privacy regimes.

0.21 Furthermore, there is increasing recognition of the unsatisfactoriness of freedom of information laws, and moves towards dedicated reviews of these by both the Commonwealth and NSW governments.²¹ Related to this is an acknowledgment that the ground is shifting under privacy and freedom of information, and the landscape may well look very different in the near future. In that case, it becomes even more important to settle high-level privacy principles that can withstand changes at the specific and detailed regulatory level.

0.22 Lastly, the timing of this report is important against the timetable of federal and State reform agendas. The federal Government will respond to the ALRC’s report in two stages, the first stage being to consider the ALRC’s recommended UPPs.²² The Government indicated its intention to finalise its response to the ALRC’s report within 12 to 18 months of its release. The Government is seeking the comments of the State and Territory governments through the Standing Committee of Attorneys-General.²³ The Government is aiming to release an exposure draft Bill by December 2009. The Commission’s views and recommendations set out in this paper are intended to contribute to the consultation phase.

21. The Commission received terms of reference on 1 June 2009 extending its terms of reference dated 11 April 2006 to encompass a review of the interaction of privacy laws with the *Freedom of Information Act 1989* (NSW). See the NSW Law Reform Commission website «<http://www.lawlink.nsw.gov.au/lrc>» at 10 September 2009.

22. Senator John Faulkner, Speech to the Cyberspace Law and Policy Centre Symposium on “Meeting Privacy Challenges – the ALRC and NSWLR Reviews”, UNSW, Sydney, 2 October 2008.

23. Senator John Faulkner, Speech to the Cyberspace Law and Policy Centre Symposium on “Meeting Privacy Challenges – the ALRC and NSWLR Reviews”, UNSW, Sydney, 2 October 2008.

0.23 New freedom of information legislation has recently been exposed or adopted in the Commonwealth, NSW and Queensland. The draft Commonwealth Information Commissioner Bill 2009 and Freedom of Information Amendment (Reform) Bill 2009 were released for public consultation on 24 March 2009. In NSW, the *Government Information (Public Access) Act 2009*, *Government Information (Information Commissioner) Act 2009* and *Government Information (Public Access) (Consequential Amendments and Repeals) Act 2009* received Assent in June 2009 and were awaiting proclamation at the time of writing. The Queensland *Right to Information Act 2009* and *Information Privacy Act 2009* commenced in July 2009.

Particular limitations

Application to public sector/private sector – impact on NSW

0.24 In DP 72, the ALRC proposed that the Privacy Act be amended to preclude State and Territory laws that regulate the handling of personal information by private sector organisations.²⁴ The implications for NSW of the Commonwealth taking over privacy regulation of organisations would be principally in relation to health information as it is only the *Health Records and Information Privacy Act 2002* (NSW) that regulates information held by organisations. The *Privacy and Personal Information Protection Act 1998* (NSW), which regulates personal information, applies only to public sector agencies. In Report 108, the ALRC went on to recommend that the Privacy Act should apply, to the exclusion of State and Territory laws, to the handling of personal information by private sector organisations.²⁵ It specifically nominated the *Health Records and Information Privacy Act 2002* (NSW) as one of the Acts that would be excluded to the extent that it applies to organisations.

0.25 In CP 3, the Commission supported the DP 72 proposal, observing that this would be highly beneficial for multi-disciplinary organisations, or those that operate across State jurisdictions, since they would only need to comply with one set of privacy principles. It would also make it easier for consumers to know which law regulates access to, and protection of, their health information.²⁶

24. ALRC DP 72 Proposal 4-1.

25. ALRC Report 108 vol 1 Recommendation 3-1.

26. NSWLRC CP 3 [4.40].

0.26 The Commission affirmed, however, that NSW would – and should – continue to have a role in regulating health information held by State public sector agencies and private sector contractors that deal with those agencies. The Commission noted that this is vital given the NSW Government’s role in the management and delivery of health care services in this State. We also noted that the ALRC acknowledges the importance of complaints-handling at a local level, and that it proposed that State and Territory complaint agencies should be delegated the power to deal with complaints concerning alleged interferences with health information privacy by private sector organisations.²⁷

0.27 Although we were supportive of the ALRC’s proposal,²⁸ and are supportive of the ALRC’s recommendation, the Commission made it clear in CP 3 that we would not make any final recommendation before obtaining the views of consumers and businesses who would be affected by handing over responsibility for health information protection in the private sector to the Commonwealth.²⁹ In the event, all submissions to CP 3 that responded to the Commission’s Proposal 5, bar one,³⁰ were in support of it.³¹

27. ALRC DP 72 Proposals 45-3 and 56-1.

28. NSWLRC CP 3 Proposal 5: “The *Health Records and Information Privacy Act 2002* (NSW) should be amended so that the handling of health information by private sector organisations is regulated under the *Privacy Act 1988* (Cth).”

29. NSWLRC CP 3 [4.42].

30. Justice Health alone opposed the proposal. It pointed out that, in the course of providing health services, there is often a linkage of health records and an exchange of health information between the private and public sectors. It was of the view, therefore, that two sets of legislation relating to health information (the *Privacy Act 1988* (Cth) for health information held by organisations and State privacy legislation for health information held by agencies), and two sets of principles to adhere to, may pose difficulties both for agencies and individuals. The Commission notes, however, that this argument loses its force in the face of the move towards adopting uniform privacy principles.

31. Australian Privacy Foundation, *Submission*; The Consumer Credit Legal Centre NSW, *Submission*; Cyberspace Law and Policy Centre, UNSW, *Submission*, 5; Inner City Legal Centre, *Submission*, 11; Office of the Privacy Commissioner, *Submission*, 5. Also, by implication but not expressly: Law Society of NSW, *Submission*, 2; Motor Accidents Authority of NSW, *Submission*; and State Records Authority of NSW, *Submission*.

0.28 Therefore, in examining each of the UPPs in the following chapters, the Commission considers whether the UPP in question effectively encompasses health information as well as personal information.

UPP1:

1. Anonymity and pseudonymity

- Introduction
- The ALRC's recommendation
- The current law in NSW
- Submissions
- The Commission's conclusions

INTRODUCTION

1.1 This chapter examines the privacy principle relating to anonymity and pseudonymity that is embodied in UPP 1, which the ALRC recommended in Report 108.¹ UPP 1 states:

UPP 1. Anonymity and Pseudonymity

Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:

- (a) not identifying themselves; or
- (b) identifying themselves with a pseudonym.

What do anonymity and pseudonymity mean?

1.2 Anonymity has been described as “a fundamental component of the right to privacy and data protection for individuals in their relations with others and the state.”² One Privacy Commissioner asserted that “anonymity is the highest right individuals should have, and it should be overruled only for justifiable reasons”.³

1.3 In *Privacy and Freedom*, one of the most influential books on privacy, Alan Westin identified anonymity as one of the four basic states of privacy. He described anonymity as occurring:

when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arena.⁴

-
1. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) vol 1 Recommendation 20-1.
 2. D H Flaherty, “Defending the Right to Anonymity”, Paper presented at the *Frontiers of Privacy* conference, Victoria, British Columbia, Canada, 13 February 2003, 1.
 3. Office of the Privacy Commissioner of Canada, *Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues* (2007) 32.
 4. A F Westin, *Privacy and Freedom* (Atheneum, 1967) 31.

1.4 In the context of dealings with agencies and organisations, anonymity has been defined as “the absence of identification data in a transaction”. A transaction is anonymous if the “specific identity of one or more of the parties to the transaction cannot be extracted from the data itself, nor by combining the transaction with other data”.⁵

1.5 Examples of instances where individuals may desire anonymity and it may be appropriate for agencies and organisations to provide such an option include when:

- making a general inquiry about a product or service, in contrast to seeking a person-specific or customised service or information;
- using counselling services, particularly where information is revealed about a third party (eg, counselling for teenage pregnancy or domestic violence); or
- “whistle-blowing”, that is, reporting misconduct.⁶

1.6 Closely related to the concept of anonymity is pseudonymity where a person’s identity is not apparent but could, under certain circumstances, be discovered. A transaction is said to be pseudonymous “if the transaction data contains no direct identifier for that person and can only be related to them in the event that specific additional data is associated with it.”⁷ Like anonymity, pseudonymity also gives an individual some control over his or her true identity. In contrast to anonymity, it enables the provider of the goods or services to identify the individual under certain circumstances.

Limitations

1.7 Anonymity cannot, of course, be absolute and should be limited by legitimate interests of protecting the public good, national security, and law and order. Identity is necessary for a myriad of dealings with agencies and organisations, for example, in order to vote, pay taxes, obtain a driver’s licence, receive welfare benefits, secure a passport, etc.

5. R Clarke, “Transaction Anonymity and Pseudonymity” (1995) 2 *Privacy Law and Policy Reporter* 88.

6. J Douglas-Stewart, *Annotated Privacy Principles* (Adelaide, Presidian Legal Publications, 3rd ed, 2007) [2-5520].

7. UK Information Commissioner’s Office, *Privacy Impact Assessment Handbook* «http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/24-technologies.html» at 10 June 2009.

Most people would also want to be uniquely identified and not be confused with others when using certain services, for example, when getting medical treatment.⁸

1.8 A democratic society that respects individual autonomy and privacy is obligated to draw the line on when and how individuals should be required to identify themselves when they participate in society. It should also recognise the legitimate interests of government and the private sector in collecting information about the identity of an individual when necessary in providing services to, or conducting business with, the individual.⁹

Anonymity as a starting point

1.9 Privacy policy on anonymity has as its starting point the entitlement of individuals not to reveal their identity, unless justified under the circumstances. Individuals should only be required to reveal their identity if this is essential to the particular transaction. Otherwise, individuals should be given the option of choosing whether or not, and how, to reveal their identity. Instead of the widespread practice of automatically collecting the identity of individuals for every dealing with organisations and agencies, anonymity should be the default position. Hence, there is a need for collectors of personal information to examine which of their dealings with individuals truly require the collection of identity.¹⁰

-
8. D H Flaherty, “Defending the Right to Anonymity”, Paper presented at the *Frontiers of Privacy* conference, Victoria, British Columbia, Canada, 13 February 2003, 3.
 9. Office of the Privacy Commissioner of Canada, *Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues* (2007) 31.
 10. See Office of the Privacy Commissioner of Canada, *Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues* (2007) 31; Information and Privacy Commissioner (Ontario, Canada) and Registratiekamer (The Netherlands), *Privacy Enhancing Technologies: The Path to Anonymity* (1995) vol 1 [1.7.5], [3.1]; D H Flaherty, “Defending the Right to Anonymity” Paper presented at the *Frontiers of Privacy* conference, Victoria, British Columbia, Canada, 13 February 2003, 1, quoting J Wouldts, former UK Deputy Data Protection Commissioner.

Precedents

1.10 A number of Australian jurisdictions have adopted an anonymity principle in their privacy statutes.¹¹ The principle in the Victorian legislation provides an example:

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.¹²

1.11 The German data protection statute offers another example by providing the following:

The design and choice of data processing systems shall be in line with the objective of collecting, processing or using no personal data, or as little as possible. In particular, the possibilities of anonymisation and pseudonymisation should be used wherever possible and when the effort required is in proportion to the desired purpose of protection.¹³

1.12 Unlike the Australian examples, the German provisions apply to both the public and private sectors, and provide for both anonymity and pseudonymity.

Technologies: threat and opportunities

1.13 A clear policy on anonymity is arguably of critical importance in an era where the rapid advances in, as well as the ever growing use of, information technologies have resulted in the enormous surge in the collection of personal information. Every time one pays for a service or product through means other than cash (eg, by credit or debit card), makes a phone call, uses the internet merely to find information or purchase products and services, etc, there is potential for an identifiable record to be created and stored in some database somewhere.¹⁴ There is a view that this development poses a serious threat to privacy and in particular, anonymity.

11. *Information Act 2003* (NT) sch 2 cl 8; *Personal Information Protection Act 2004* (Tas) sch 1 cl 8; *Information Privacy Act 2000* (Vic) sch 1, cl 8.

12. *Information Privacy Act 2000* (Vic) sch 1, cl 8.

13. *Federal Data Protection Act 1990* (Germany) art 3a.

14. Information and Privacy Commissioner (Ontario, Canada) and Registratiekamer (The Netherlands), *Privacy Enhancing Technologies: The Path to Anonymity* (1995) vol 1 [1.0].

1.14 There are, however, existing technologies that allow anonymous transactions. One class of technologies, which rely on a succession of intermediary-operated services, has been described as follows:

Each intermediary knows the identities of the intermediaries adjacent to it in the chain, but has too little information to enable it to identify the prior and subsequent intermediaries. Even if it wants to, it cannot track the communication back to the originator or forward to the ultimate recipient. Examples ... include anonymous remailers, web-surfing arrangements, and ... payer-anonymous ECash or Digicash.¹⁵

1.15 However, technologies that provide genuine anonymity give rise to concerns about accountability. The inability of agencies and organisations to trace identity heightens the risk for individuals to commit unlawful activity, such as fraud.¹⁶ An alternative to anonymity is pseudonymity where a person's identity is not apparent but could, under certain circumstances, be discovered. Examples of techniques that can be integrated in information systems of service providers (agencies and organisations) for the purpose of allowing pseudonymous transactions include:

- digital pseudonym, which the service provider assign to a customer, for the purposes of conducting transactions; and
- trusted third party, which is a party charged with keeping the master key linking digital pseudonyms with the true identities of their users. Only certain conditions (which are agreed upon by the parties) will allow the trusted party to reveal a user's identity to the service provider.¹⁷

1.16 Hence, just as technology has facilitated the explosive growth in the collection of personal information which threatens privacy, technology can be used to protect privacy in an electronic age.¹⁸

15. R Clarke, "Introducing PITs and PETs: Technologies Affecting Privacy" (2001) 7 *Privacy Law & Policy Reporter* 181, 182.

16. R Clarke, "Introducing PITs and PETs: Technologies Affecting Privacy" (2001) 7 *Privacy Law & Policy Reporter* 181, 183.

17. See Information and Privacy Commissioner (Ontario, Canada) and Registratiekamer (The Netherlands), *Privacy Enhancing Technologies: The Path to Anonymity* (1995) vol 2 [4.0].

18. Office of the Privacy Commissioner of Canada, *Identity, Privacy and the Need of Others To Know Who You Are: A Discussion Paper on Identity Issues* (2007) 44.

THE ALRC'S RECOMMENDATION

The current Commonwealth law

1.17 The Principles contained in the Privacy Act, which agencies¹⁹ must observe, do not include obligations of anonymity or pseudonymity.

1.18 In contrast, NPP 8 of the Privacy Act, which applies to organisations,²⁰ states:

Whenever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

1.19 In Report 108, the ALRC examined:

- whether the anonymity principle embodied in NPP 8 should cover agencies in addition to organisations;
- whether the principle should be expanded to cover pseudonymity; and
- what should be the content of this principle.²¹

Extension of the anonymity principle to agencies

1.20 The ALRC recommended that an anonymity principle should be included in the model UPPs and should apply equally to agencies and organisations. It reasoned that an anonymity principle would encourage agencies and organisations to consider the fundamental question of whether they need to collect personal information at all and to design their systems accordingly.²² In other words, such a principle may assist in minimising the collection of unnecessary personal information.²³

19. See *Privacy Act 1988* (Cth) s 13(a), 16.

20. *Privacy Act 1988* (Cth) s 16A. Organisations for purposes of the *Privacy Act 1988* (Cth) covers individuals, corporations, unincorporated associations, partnerships and trusts, but *excludes*: small businesses, political parties, state/territory authorities and agencies to which the Principles apply: *Privacy Act 1988* (Cth) s 6C.

21. ALRC Report 108 vol 1 [20.5].

22. ALRC Report 108 vol 1 [20.14].

23. Privacy NSW, *Submission PR 468*, 14 December 2007 cited in ALRC Report 108 vol 1 [20.8].

1.21 Further, the ALRC said that providing individuals greater control over their privacy by giving them the option to transact anonymously, where appropriate, may give rise to significant public policy benefits. It may, for example, encourage individuals to seek medical or other services from an organisation or agency in situations where a requirement of identification would discourage them from seeking such services. The ALRC cited as illustration the anonymous supply of sterile syringes and needles to injecting drug users, which it said is an important public health initiative in all Australian States and Territories.²⁴

1.22 A number of agencies expressed concerns about the practical application of an anonymity principle. The ALRC said that these could be accommodated adequately within the broad limitations of the principle — that is, that the option for anonymity must be provided only where it is “lawful and practicable”. This issue is discussed in greater detail below.²⁵

Pseudonymity

1.23 The ALRC recommended that the anonymity principle should provide for pseudonymous transactions, that is, where appropriate, agencies and organisations should give an individual the option of using a name (other than his or her real name), term or other combination of letters and numerals by which he or she can be addressed specifically.²⁶

1.24 The ALRC expressed the view that provision for pseudonymity would bestow:

a more flexible application of the principle by covering the situation where it would be impracticable or unlawful for an individual to transact anonymously but where these barriers would be overcome if the individual were to transact pseudonymously with an agency or organisation. An extension of the principle to encompass pseudonymous transactions will also encourage agencies and organisations to incorporate into their systems privacy-enhancing technologies that facilitate pseudonymous interactions in an online environment.²⁷

24. ALRC Report 108 vol 1 [20.14].

25. See para 1.29-1.39.

26. ALRC Report 108 vol 1 [20.17].

27. ALRC Report 108 vol 1 [20.25].

1.25 There were, however, two main objections that came out of the submissions, namely:

- the cost of implementation could be high; and
- pseudonymous transactions are open to abuse and may detract from the accuracy of records.

1.26 The ALRC acknowledged these concerns but said that they can be accommodated adequately within the broad limitations of the proposed principle, that is, transacting anonymously or pseudonymously must be “lawful and practicable”.²⁸

1.27 The Office of the Federal Privacy Commissioner (“OPC”), which supports the inclusion of pseudonymity within the anonymity principle, raised concerns that agencies and organisations might use the terms pseudonymity and anonymity interchangeably and consequently only offer one of the options to individuals. It suggested that:

the wording of the principle [should] be clarified to ensure that organisations and agencies provide individuals with the option of interacting anonymously where this is lawful and practicable. Where it is not practicable for an individual to transact anonymously or where the individual chooses to transact under a pseudonym an agency or organisation [should be] required to give individuals the clear option to transact pseudonymously if this is lawful and practicable.²⁹

1.28 The ALRC was not, however, convinced that UPP 1 should expressly provide for a calibrated approach to anonymity and pseudonymity. It considered that the decision of an agency or organisation to give individuals an option to interact anonymously or pseudonymously would be guided by the particular context. Further, it said that the OPC should provide guidance on matters that an agency or organisation ought to consider when deciding whether to provide an option for anonymity or pseudonymity.³⁰ Nevertheless, it expressed the view that, as a general rule, where the agency or organisation has no need to contact the individual in the future, anonymity would be the most appropriate option. Where an identifier is required for a transaction but

28. ALRC Report 108 vol 1 [20.25].

29. Office of the Federal Privacy Commissioner, *Submission PR 499*, 20 December 2007 cited in ALRC Report 108 vol 1 [20.23]-[20.24].

30. See ALRC Report 108 vol 1 Recommendation 20-2.

there is no need for disclosure of personal information, pseudonymity is likely to be appropriate.³¹

Content and application

Lawful and practicable

1.29 A considerable number of agencies and organisations expressed concerns in their submission to the ALRC about the practical application of an anonymity and pseudonymity principle.

1.30 For example, the ACT Department of Disability Housing and Community Services said that, in relation to the provision of services to children at risk of abuse or neglect, the identification of the persons involved is essential in the recording of client history, which is an important part of risk assessment and in deciding appropriate services for the children concerned.³²

1.31 The Australian Government Department of Human Services advised that it cannot provide full and reliable advice to an individual who remains anonymous or provides a pseudonym.³³

1.32 The Department of Foreign Affairs and Trade expressed disquiet about the potential compliance costs, for example, with respect to the amendment of the Department's online forms, including passport applications.³⁴

1.33 The submissions also identified situations where the application of an anonymity and pseudonymity principle could conflict with legislative requirements to retain identifying information, including those that apply to the telecommunications industry, the provision of health care and health insurance, and the financial services sector.³⁵

31. Office of the Federal Privacy Commissioner, *Submission PR 499*, 20 December 2007 cited in ALRC Report 108 vol 1 [20.27].

32. ALRC Report 108 vol 1 [20.32].

33. ALRC Report 108 vol 1 [20.33].

34. ALRC Report 108 vol 1 [20.34].

35. ALRC Report 108 vol 1 [20.35].

1.34 Some submissions suggested that specific exceptions be provided, for example for the delivery of health benefits and social services by Commonwealth agencies, or for the provision of health care.³⁶

1.35 The ALRC, however, emphasised that the requirement in UPP 1 for agencies and organisations to give individuals the options of anonymity and pseudonymity is not absolute since it arises only where this is “lawful and practicable”. This is based on the similarly-worded qualification found in NPP 8.³⁷

1.36 In relation to NPP 8, a commentator has said that it would not be lawful for an organisation to give an individual the option of transacting anonymously if a law requires the organisation to identify the individual, for example, to open a bank account or for reporting requirements regarding a notifiable disease or suspected child abuse.³⁸

1.37 Further, for the purpose of determining whether it is “practicable” for an organisation to deal anonymously with an individual, the same commentator suggested that the following factors may be taken into account:

- whether the provision of the product or service requires the individual to be identified;
- whether the provision of the product or service could be improved if the individual’s identity was known (for example in relation to a health service where the review of the patient’s medical record may assist in treatment);
- whether there will be an increase in cost or time involved in providing the product or service; and
- whether there will be increased risk to the organisation in providing the product or service anonymously (for example, in the event of legal proceedings, the organisation may not be able to provide evidence of correspondence with the individual).³⁹

36. ALRC Report 108 vol 1 [20.36].

37. Para 1.18.

38. J Douglas-Stewart, *Annotated Privacy Principles* (Adelaide, Presidian Legal Publications, 3rd ed, 2007) [2-5530].

39. J Douglas-Stewart, *Annotated Privacy Principles* (Adelaide, Presidian Legal Publications, 3rd ed, 2007) [2-5540].

1.38 The ALRC concluded that the “lawful and practicable” qualification to the proposed anonymity and pseudonymity principle would adequately address the concerns raised in the submissions. Further, it said that there is no need to give specific agencies or organisations exemption from the proposed principle. It asserted that the question of whether the principle should apply would depend on the nature of the particular context. It expressed the view that, where an agency is doing an activity directly related to the provision of a government benefit, it generally will not be “lawful and practicable” for the agency to offer an option of anonymity or pseudonymity. In contrast, where the agency is undertaking a more generic interaction with the public, such as giving information on general departmental policy or procedure, anonymity or pseudonymity may be appropriate.⁴⁰

1.39 The ALRC recommended that the OPC issue guidance on the “lawful and practicable” requirement.⁴¹

Not misleading

1.40 In its DP 72,⁴² the ALRC proposed that the option to transact pseudonymously should be subject to the additional limitation that it would not be misleading.⁴³ The ALRC was concerned about the potential for pseudonymous transactions to lead to fraudulent or misleading practices. Although fraud would be adequately covered by the requirement that the transaction be “lawful”, the ALRC was worried that, in certain situations, a pseudonymous transaction may be misleading but not necessarily fraudulent. It gave the example of an individual who intentionally chooses as a pseudonym someone else’s name for the purpose of giving the impression that he or she is actually that other person.⁴⁴

1.41 In Report 108, however, the ALRC acknowledged that agencies and organisations might find it onerous to apply a requirement that a pseudonym not be misleading. For example, they are likely to find it difficult to assess an individual’s intentions when he or she interacts

40. ALRC Report 108 vol 1 [20.46].

41. ALRC Report 108 vol 1 Recommendation 20-2 [20.43].

42. Australian Law Reform Commission, *Review of the Law of Privacy*, Discussion Paper No 72 (2007) (“ALRC DP 72”).

43. ALRC DP 72 Proposal 17-2.

44. ALRC DP 72 vol 2 [17.23].

pseudonymously. The ALRC concluded that the requirement that the pseudonymous interaction must be “lawful and practicable” is sufficient to guard against systemic abuse.⁴⁵

“Interacting” with individuals

1.42 The current anonymity principle embodied in NPP 8 refers to individuals’ option of not identifying themselves “when entering transactions” with an organisation.

1.43 The OPC submitted that this should be amended to clarify that, where an individual has an existing relationship with an organisation, that individual is still entitled to transact anonymously, subject to relevant qualifications.⁴⁶

1.44 In its DP 72, the ALRC agreed that the clarification suggested by the OPC should be incorporated into its proposed anonymity and pseudonymity principle by replacing the words “when entering transactions” with the words “when transacting”.⁴⁷

1.45 In Report 108, however, the ALRC decided to replace the word “transacting” with “interacting”. It reasoned that since, on its plain English meaning, “interact” has a wider import than “transact”, the use of “interacting” would more clearly establish that the proposed principle is intended to cover a broad range of dealings. It was concerned that “the term ‘transacting’ may be associated unduly with customised transactions or service delivery, where anonymity or pseudonymity will often not be appropriate”.⁴⁸

“Clear option”

1.46 The current anonymity principle found in NPP 8 provides that “individuals must have the option of not identifying themselves”. The ALRC queried whether the proposed extension of this principle might be better drafted by imposing expressly an obligation on agencies and organisations to give individuals the option to interact anonymously and

45. ALRC Report 108 vol 1 [20.48] [20.49].

46. ALRC DP 72 vol 2 [17.24].

47. ALRC DP 72 vol 2 [17.25].

48. ALRC Report 108 vol 1 [20.42].

pseudonymously.⁴⁹ The anonymity principle in the Northern Territory legislation, for example, provides the following:

A public sector organisation must give an individual entering transactions with the organisation the option of not identifying himself or herself unless it is required by law or it is not practicable that the individual is not identified.⁵⁰

1.47 The ALRC concluded that the anonymity and pseudonymity principle should be drafted in a way that clarifies that the onus is on agencies and organisations to give individuals the options to interact anonymously and pseudonymously.⁵¹ It examined two reform choices for this purpose, namely, requiring agencies and organisations to provide either an *express* option or a *clear* option to individuals to transact anonymously or pseudonymously.

1.48 It described an express option as requiring an agency or organisation to state explicitly (for example, on its information collecting system) that individuals may transact anonymously or pseudonymously. In contrast, a clear option would merely require the agency or organisation to ensure that individuals are aware that they may transact anonymously or pseudonymously.⁵²

1.49 It considered a requirement to provide individuals with a clear option as less onerous than a requirement to provide an express option. It said that such a requirement

would allow agencies and organisations to comply with the ‘Anonymity and Pseudonymity’ principle in the *structure* of their information collecting systems. For example, in many cases where asked to fill out a form either on paper or electronically, individuals are told which fields they must complete. Providing a clear option may entail altering the list of ‘required fields’ to take account of the ‘Anonymity and Pseudonymity’ principle. An express option may require agencies and organisations to undertake an additional step of notifying individuals that they do not need to complete the fields containing identifying information.⁵³

49. Australian Law Reform Commission, *Review of Privacy*, Issues Paper No 31 (2006), Issue 4-29.

50. *Information Act 2002* (NT) sch 2 cl 8.

51. ALRC Report 108 vol 1 [20.64].

52. ALRC Report 108 vol 1 [20.57].

53. ALRC Report 108 vol 1 [20.58].

1.50 It concluded that “requiring agencies and organisations to provide individuals with a clear option of interacting anonymously or pseudonymously represents an appropriate balance between the interest in making individuals aware of their option to not identify themselves, or identify themselves pseudonymously, and the need to limit the cost of compliance for agencies and organisations”.⁵⁴

1.51 The ALRC’s recommended anonymity and pseudonymity principle required “an agency or organisation to give individuals the clear option to interact anonymously or pseudonymously, where this is lawful and practicable in the circumstances”.⁵⁵

THE CURRENT LAW IN NSW

1.52 PPIPA does not have a principle on anonymity.

1.53 In contrast, HRIPA contains a principle — HPP 13 — which states:

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.⁵⁶

1.54 HPP 13 reflects NPP 8 of the Privacy Act, which, as mentioned earlier, is the basis of the ALRC recommendation.

SUBMISSIONS

1.55 The Commission’s CP 3⁵⁷ did not specifically deal with the anonymity principle. Nevertheless, two submissions support such a principle. In response to the question we posed of whether NSW should continue to have two separate information privacy statutes, the Australian Privacy Foundation and the Cyberspace Law and Policy Centre answered in the negative but qualified that PPIPA (or the privacy legislation that is eventually adopted for NSW) should contain a number of additional principles, including one on anonymity.⁵⁸

54. ALRC Report 108 vol 1 [20.62].

55. ALRC Report 108 vol 1 Recommendation 20-1.

56. *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 13.

57. NSW Law Reform Commission, *Privacy Legislation in New South Wales* Consultation Paper No 3 (2008).

58. Australian Privacy Foundation, *Submission*, 3; Cyberspace Law and Policy Centre, *Submission*, 6.

THE COMMISSION'S CONCLUSIONS

1.56 The Commission supports adopting UPP 1 into State privacy legislation. Anonymity is an important aspect of privacy and individuals should only be required to reveal their identity if this is essential to the particular transaction. The recommended principle would give individuals greater control over their privacy by giving them the option of interacting with government anonymously or pseudonymously, where this is lawful and practicable. It would also encourage agencies to examine which of their interactions with the public truly require the collection of identity, and this should assist in curbing the propensity by government to automatically collect the identity and other personal information of individuals even in situations where it is unnecessary to do so.

1.57 The Commission agrees with the terms of the ALRC's recommendation, including the provision for agencies to give individuals the option of interacting pseudonymously. This would give agencies flexibility in situations where it would be unlawful or impracticable for an individual to interact anonymously but where these barriers would be overcome if the individual were to transact pseudonymously with the agency. Pseudonymity still gives an individual control over his or her true identity but also ensures that the individual remains accountable by enabling the agency to trace his or her identity under certain circumstances, for example where unlawful activity has been committed.

1.58 An important element of the recommended principle is the qualification that agencies provide individuals with the option of anonymity or pseudonymity where this is "lawful and practicable". This recognises that individuals' interest in anonymity and pseudonymity is not absolute. The qualification is capable of encompassing a broad range of situations, such as where identification is required by law or by the nature of the interaction.

1.59 There is a clear need to clarify how the principle would operate, particularly with respect to when anonymous and pseudonymous interactions would be appropriate, and when the "lawful and practicable" qualification would apply. Agencies would require, for example, directions on what factors they should take into account when determining whether it is "practicable" for them to interact with an individual. There is also a need for guidance on

- what is involved in providing a “clear option” to interact anonymously or pseudonymously; and
- the difference between providing individuals with the option to interact anonymously and pseudonymously.

1.60 We agree with the ALRC that these are matters for clarification through guidance to be developed by the Privacy Commissioner.⁵⁹

59. See ALRC Report 108 vol 1 Recommendation 20-2.

2. UPP 2: Collection

- Introduction
- Purposes of collection
- Means and manner of collection
- Collection from the individual concerned
- Unsolicited personal information
- Sensitive information

INTRODUCTION

2.1 This chapter examines UPP 2, which the ALRC recommended as the model privacy principle on the collection of personal information.

2.2 The first part of the chapter analyses UPP 2.1 to 2.4, which contain the rules that apply generally to the collection of personal information.

2.3 The second part of the chapter examines UPP 2.5 and 2.6, which contain provisions that apply specifically to the collection of categories of personal information that have been defined as sensitive information under the Privacy Act.

2.4 For reading convenience, the provisions of UPP 2.1 to 2.4 are reproduced here, while UPP 2.5 and 2.6 are quoted later in the chapter.¹

UPP 2. Collection

2.1 An agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.

2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

2.3 If it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual.

2.4 If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either:

- (a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or
- (b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had actively collected the information.

1. See para 2.81.

PURPOSES OF COLLECTION

The ALRC's recommendation

2.5 Principle 1 of the Privacy Act provides that an agency may only collect personal information if the:

- information is collected for a lawful purpose directly related to a function or activity of the agency; and
- collection of that information is necessary for, or directly related to, that purpose.

2.6 NPP 1, the counterpart of Principle 1 which applies to organisations, provides that an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

2.7 The ALRC, in Report 108, recommended that the collection principle in the UPPs “should provide that an agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities”.² This recommendation is found in UPP 2.1

2.8 The ALRC used NPP 1 as the template for UPP 2.1. It noted that NPP 1 is simpler in form than Principle 1.³ Further, it observed that the requirement in NPP 1 that an organisation must not collect personal information unless it is “necessary for one or more of its functions or activities” implies an objective test, that is, “the collection has to be necessary, not necessary merely in the opinion of the organisation”.⁴ It asserted that an “objective test should encourage organisations and agencies to give careful consideration to whether the personal information they collect is genuinely necessary for their functions or activities”.⁵

2.9 The ALRC's final recommendation may be compared with its proposal in DP 72, which stated that the collection principle in the model

2. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) vol 1 Recommendation 21-5.

3. ALRC Report 108 vol 1 [21.76].

4. ALRC Report 108 vol 1 [21.75].

5. ALRC Report 108 vol 1 [21.74].

UPPs should provide that an agency or organisation must not collect personal information unless it reasonably believes the information is necessary for one or more of its functions or activities.⁶ The ALRC acknowledged in Report 108 that a number of submissions expressed concern that, under the original proposal, what is necessary for the functions or activities of an agency or organisation is determined by the subjective belief of the agency or organisation. The submissions preferred an objective test and the ALRC agreed with such view.⁷

2.10 Consequently, the ALRC removed the subjective test in its original proposal. It did not, however, consider it necessary for UPP 2.1 to expressly provide that the collection must be *reasonably* necessary for one or more of the collector's functions or activities, and that the perspective of the reasonable person is to be applied in determining the necessity of the collection. It opined that these requirements are already implied by the terms of UPP 2.1.⁸

2.11 Further, the ALRC said that it is unnecessary to provide expressly that the purpose of collection should be lawful and objectively reasonable. It argued that its recommendation implies that: (1) the activities and functions pursuant to which agencies and organisations collect personal information must be lawful; and (2) such collection pursuant to those functions must be lawful. It declared that the collection principle does not, and cannot, make unlawful collections lawful, for example, where an agency collects information beyond the scope of its powers.⁹

The current law in NSW

2.12 Section 8 of PPIPA provides that a public sector agency must not collect personal information unless:

- the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and
- the collection of the information is reasonably necessary for that purpose.

6. Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No 72 (2007) Proposal 18-3 ("ALRC DP 72").

7. ALRC Report 108 vol 1 [21.72].

8. ALRC DP 72 Proposal 18-3.

9. ALRC Report 108 vol 1 [21.77].

2.13 The parallel principle in HRIPA — HPP 1 — is almost identical to s 8 of PIPPA. HPP 1 provides that an organisation must not collect health information unless:

- the information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and
- the collection of the information is reasonably necessary for that purpose.¹⁰

The Commission's conclusions

2.14 The Commission supports UPP 2.1, subject to some suggestions discussed below. The provisions of UPP 2.1 simplify but still capture the essence of the current NSW privacy principles that an agency must not collect personal information unless it is necessary for one or more of its functions or activities.

2.15 The Commission agrees with the view expressed by the ALRC that it is unnecessary to provide expressly that the purpose of collection should be lawful. A collection principle based on UPP 2.1 implies that the activities and functions pursuant to which agencies and organisations may collect personal information must be lawful, and such collection pursuant to those functions must be lawful.

2.16 The Commission, however, differs with the ALRC regarding the provision of a test for the necessity of the collection. The Commission is of the view that UPP 2.1 should — like s 18 of PPIPA — provide that the collector of the collection of personal information may collect the information if the collection is *reasonably* necessary for one or more of its functions or activities. Further, there should be express provision (not necessarily in UPP 2.1) that an objective test is to be used in determining whether the collection is reasonably necessary under the circumstances. An express provision would give clarity and certainty for agencies that they may only collect personal information that is necessary for their functions or activities, not information that they reasonably believe may be necessary for their functions or activities. It should induce them to give judicious consideration to whether the personal information they collect is genuinely necessary for their functions or activities. Further, an express provision would better inform individuals about the test by which their

10. *Health Records and Information Privacy Act 2002* (NSW) sch 1, HPP 1.

personal information may be legitimately collected, which may enable them to challenge any inappropriate collection.

2.17 The *Personal Information Protection Act* of the Canadian province of Alberta offers a reform model on this matter. Section 11 of this Act states the principle on the collection of personal information in the following manner:

- (1) An organization may collect personal information only for purposes that are reasonable.
- (2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.

2.18 Section 2 of the Act provides the test for what is reasonable under this section and other provisions of the Act, thus:

Where in this Act anything or any matter

- (a) is described, characterized or referred to as reasonable or unreasonable, or
- (b) is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner,

the standard to be applied under this Act in determining whether the thing or 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.

2.19 The Commission finds the approach in the Alberta statute appropriate for purposes of the Privacy Act and the State privacy legislation that will contain the UPPs. References to reasonable or unreasonable matters are not confined to UPP 2.1 but can be found in a fair number of UPPs. Some UPPs, for example, contain a “reasonable and practicable” or “lawful and reasonable” or “unreasonable impact”¹¹ qualification or exception,¹² or refer to the taking of “reasonable steps”,¹³ or compliance within a “reasonable time”.¹⁴ The inclusion of a section similar to the Alberta statutory provisions quoted above would clarify the

11. UPP 9.1(c).

12. UPP 2.4(a), UPP 2.3, UPP 2.5(f)(ii), UPP 5.1(g)(i), UPP 6.2(d), UPP 9.5.

13. UPP 2.6, UPP 3, UPP 4.2, UPP 7, UPP 8.1, UPP 9.3, UPP 9.6, UPP 9.7(b).

14. UPP 9.1.

standard to be applied in determining whether the matter referred to in the relevant UPPs is reasonable or unreasonable.

RECOMMENDATION 1

UPP 2.1 should be modified as follows:

2.1 An agency or organisation must not collect personal information unless it is *reasonably* necessary for one or more of its functions or activities.

RECOMMENDATION 2

The 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.

MEANS AND MANNER OF COLLECTION

2.20 The ALRC's recommended UPP on collection contains the following provision on the means and manner of collecting personal information:

An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.¹⁵

2.21 This provision, which is found in UPP 2.2, was not the subject of a specific discussion in the ALRC report. It appears to be based on NPP 1.2, which is similarly worded.

2.22 In NSW, PPIPA contains the following relevant provisions:

- Section 8(2) provides that a public sector agency must not collect personal information by any unlawful means.

15. ALRC Report 108 vol 1 [21.83].

- Section 11(b) provides that, if a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

2.23 The HPPs contain similar provisions.¹⁶

2.24 UPP 2.2 should be adopted in NSW. It would simplify the NSW provisions and strengthen the safeguards on the collection of personal information by requiring that the means used for such collection be lawful as well as *fair*.

COLLECTION FROM THE INDIVIDUAL CONCERNED

The ALRC's recommendations

2.25 The current Principles on collection of personal information (Principles 1-3) do not impose a requirement on agencies to collect information directly from an individual.

2.26 In contrast, NPP 1 requires organisations, where reasonable and practicable, to collect personal information about an individual only from that individual.

2.27 The ALRC, in Report 108, recommended that the collection principle should require agencies and organisations, where reasonable and practicable, to collect personal information about an individual only from the individual concerned.¹⁷ This recommendation is embodied in UPP 2.3.

16. HPP 1(2) states that an organisation must not collect health information by any unlawful means. HPP 2(b) provides that an organisation that collects health information from an individual must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates: see *Health Records and Information Privacy Act 2008* (NSW) sch 1.

17. ALRC Report 108 vol 1 Recommendation 21-1.

2.28 It reasoned that its recommendation would increase the likelihood that personal information collected will be accurate, relevant, complete and up-to-date. Further, it said that the recommendation would give individuals an opportunity to participate in the collection process.¹⁸

2.29 The ALRC emphasised that a requirement to collect personal information about an individual exclusively from the individual concerned would apply only “where reasonable and practicable”. It indicated that there would be many circumstances where it will not be reasonable or practicable to collect personal information directly from the individual concerned. It will *not* be reasonable and practicable, for example, to collect personal information directly from an individual where direct collection would prejudice the purpose of collection, such as where a law enforcement body is investigating a breach of a criminal law. It said that the requirement is not intended to limit the coercive information-gathering powers of agencies, or the exercise of their intelligence, investigative and compliance functions.¹⁹

2.30 The ALRC also recommended that the Office of the Privacy Commissioner, Australia (“OPC”) should develop and publish guidance to clarify when it would not be reasonable and practicable to collect personal information about an individual only from the individual concerned. In particular, the guidance should address collection:

- of personal information by agencies pursuant to the exercise of their coercive information-gathering powers or in accordance with their intelligence-gathering, investigative, and compliance functions;
- of statistical data;
- of personal information in circumstances in which it is necessary to verify an individual’s personal information;
- of personal information in circumstances in which the collection process is likely to, or will, disclose the personal information of multiple individuals; and

18. ALRC Report 108 vol 1 [21.31].

19. ALRC Report 108 vol 1 [21.32].

- from persons under the age of 18, persons with a decision-making incapacity and those authorised to provide personal information on behalf of the individual.²⁰

The current law in NSW

2.31 Section 9 of PPIPA, which is titled “Collection of personal information directly from individual”, states:

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:

- (a) the individual has authorised collection of the information from someone else, or
- (b) in the case of information relating to a person who is under the age of 16 years — the information has been provided by a parent or guardian of the person.

2.32 Unlike UPP 2.3, s 9 of PPIPA does not have a “where reasonable and practicable” qualification.

2.33 HPP 3, which is titled “Collection to be from individual concerned”, provides:

- (1) An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.
- (2) Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.²¹

20. ALRC Report 108 vol 1 Recommendation 21-2.

21. The NSW Privacy Commissioner has issued guidelines pursuant to HPP 3(2). The guidelines provide some examples of when it may be unreasonable or impracticable to collect health information directly from the person concerned, including, among others: (a) where a person is admitted unconscious to an emergency ward; (b) where a person lacks the capacity to provide his or her health information; and (c) in the course of taking the family, social or medical history of a patient, if this is relevant to providing the health service to the patient: Office of the NSW Privacy Commissioner, *Handbook to Health Privacy* (2004) 21-22.

2.34 The provisions of HPP 3 are similar to those of UPP 2.3, particularly in regard to the inclusion of an “unreasonable or impracticable” qualification.

Submissions

2.35 In CP 3, the Commission proposed that (assuming NSW would adopt a single privacy Act containing the privacy principles) the principle governing collection of personal information directly from an individual should contain the two exceptions currently provided for in s 9 of PPIPA, as well as the third exception currently provided for in HPP 3, namely, that information must be collected from the individual unless it is “unreasonable or impractical to do so”.²²

2.36 The Australian Privacy Foundation and the Cyberspace Law and Policy Centre supported this proposal.²³

2.37 The NSW Department of Community Services (“DOCS”) and the NSW Department of Ageing, Disability and Home Care were particularly supportive of the proposed “unreasonable and impractical” exception. DOCS noted that such an exemption is found in NPP 1 and in the privacy principles for public sector agencies in Victoria, Tasmania and the Northern Territory.²⁴

2.38 There was, however, apprehension about the scope of the “unreasonable and impracticable” qualification. The Inner City Legal Centre (“ICLC”) expressed concern that the proposed exception could be “interpreted expansively and would be guided by the subjective operational needs of the organisation in question rather than an objective application”. It suggested that the proposed qualification be recast in the following manner:

unreasonable or impractical to do so by reasons of the person’s incapacity to give the information or consent to indirect collection, and the information is necessary for the provision of beneficial services, diagnosis, treatment or care in respect of the individual.

22. NSW Law Reform Commission, *Privacy Legislation in New South Wales* Consultation Paper No 3 (2008) (“NSWLRC CP 3”) Proposal 8.

23. Australian Privacy Foundation, *Submission*, 8; Cyberspace Law and Policy Centre, *Submission*, 20.

24. NSW Department of Community Services, *Submission*, 5-6; NSW Department of Ageing, Disability and Home Care, *Submission*, 2.

2.39 The ICLC contended that such an approach would enhance the privacy of the individual, while the current proposal would shift the balance too much in favour of bureaucratic expedience.²⁵

2.40 The Public Interest Advocacy Centre also said that the proposed “reasonable and practicable” exception may be too broad. It preferred the concept of “unjustifiable hardship” under anti-discrimination laws, which it considered to be the less permissive and more objective. It suggested that the collection principle provide that personal information may be collected from the individual unless it would impose unjustifiable hardship on the collector.²⁶

2.41 The NSW Minister for Housing underlined the importance of the exception on authorisation by the individual under s 9 of PPIPA. She considered it appropriate for personal information to be collected from a third party if the person to whom the information relates consents. She said that there are many instances where her Department needs to collect personal information indirectly, for example, where the Department requires information from a medical practitioner about the mental health of an applicant for priority housing.²⁷ The consent exception allows the Department to ask in the application form whether the applicant consents to the Department obtaining relevant personal information from other persons, agencies or organisations.

The Commission’s conclusions

2.42 Section 9 of PPIPA imposes two bright-line tests. If either of those tests is satisfied, no further test of either unreasonableness or impracticability of collecting the information from the individual must be satisfied; that is, the agency simply has power, even if it would be neither unreasonable nor impracticable to collect the information directly from the individual.

2.43 In comparison, UPP 2.3 imposes no bright-line test but rather two tests (unreasonableness and impracticability), each of which requires the making of an evaluative judgment. Each of those tests has the potential to empower the collection of personal information otherwise than from the individual to whom the information relates in circumstances where the

25. Inner City Legal Centre, *Submission*, 13-14.

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

27. Minister for Housing, *Submission*, 2.

collection is not empowered by s 9 of PPIPA. However, neither of those tests will necessarily be satisfied where the individual concerned has authorised the collection of the information from someone else or is under the age of 16 years.

2.44 The ALRC recommended that the OPC issue guidance on the unreasonableness and impracticability tests. The issue that arises is whether the two exceptions under s 9 of PPIPA can be covered through the recommended OPC guidance. This would depend on whether the recommended OPC guidance would be binding or non-binding.

2.45 The nature of recommended OPC guidance is not clear but it would appear that they are intended to be non-binding.²⁸ In Report 108, the ALRC distinguished “guidelines” from “rules”. It described guidelines as providing a “voluntary guide on ways to achieve the outcome set by the relevant privacy principle, without compelling directly a particular course of action”. In contrast, rules are binding and their breach “constitutes an interference with privacy”.²⁹ It maintained this distinction in its recommendations by using the term “rules” when it wants the OPC to issue guidance that is binding.³⁰ The fact that the ALRC did not use the word “rules” in its recommendation for the OPC to issue guidance on the unreasonable and unreasonable tests under UPP 2.3 indicates that such guidance is intended to be non-binding. Consequently, the OPC guidance would provide no guarantee that information could be collected from third parties in circumstances now covered by s 9 of PPIPA.

2.46 The Commission is of the view that the exception in s 9 of PPIPA relating to an individual authorising an agency to collect his or her personal information from someone else should be included as one of the exceptions in UPP 2.3. Individuals should be given autonomy with respect to how their personal information may be collected. Where, for example, an individual decides to acquiesce to a request for his or her personal information to be collected from someone else, or simply considers such mode of collection convenient, the law should sanction such collection, even if it would be reasonable or practicable for the

28. For a general discussion on guidance pursuant to the Privacy Act, see ALRC Report 108 vol 1 [47.25]-[47.36].

29. ALRC Report 108 vol 1 [47.36].

30. See, for example, para 2.129-2.130.

agency or organisation to collect the information from the individual. The main concern of the ALRC in limiting the number of exceptions in UPP 2 and other UPPs is to ensure that the privacy principles are not too detailed and prescriptive so as to remain consistent with the high-level principles approach it adopted in crafting the UPPs.³¹ The Commission considers that the addition of the one more exception in UPP 2.3 will not detract from the ARLC's approach.

2.47 The other exception in s 9 of PPIPA — personal information relating to a person who is under the age of 16 years — need not be added as an exception to UPP 2.3 because it can be dealt with through the unreasonable or impracticable exception. An example might be where an agency or organisation needs information relating to a 13-year old child, who does not have the legal capacity to disclose the information.³² It is arguable that since it is legally impracticable to collect the information from the child, collection from someone else (that is, a person having parental responsibility for the child) would be authorised under UPP 2.3.

RECOMMENDATION 3

UPP 2.3 should be revised to read as follows:

2.3 An agency or organisation may collect personal information otherwise than directly from the individual to whom the information relates when either:

- the individual has authorised the collection of the information from someone else; or
- collection from the individual is not reasonable or practicable under the circumstances.

UNSOLICITED PERSONAL INFORMATION

2.48 Agencies and organisations very often receive unsolicited personal information. This occurs when personal information is given to an agency or organisation that did not take active steps to collect that information.

31. See ALRC Report 108 vol 1 Ch 18. See also para 0.5-0.9.

32. See *Health Records and Information Protection Act* s 7 (an individual is incapable of doing an act authorised, permitted or required by this Act 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).

The ALRC's recommendations

2.49 At the Commonwealth level, the Principles, to some limited extent, distinguish between the obligations imposed on an agency when soliciting personal information, on the one hand, and when receiving unsolicited personal information, on the other hand. Principles 2 and 3 impose certain obligations on an agency only where it has solicited personal information. The obligations in Principle 1, however, do not refer expressly to solicited information and were intended to apply where an agency receives unsolicited material, for example, from sources such as a ministerial letter or a tip-off from an informer.³³

2.50 The NPPs do not distinguish between obligations of an organisation relating to solicited and unsolicited information.

2.51 The ALRC, in Report 108, recommended that the collection principle should provide that, where an agency or organisation receives unsolicited personal information, it must either:

- if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or
- comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.³⁴

2.52 Under this recommendation, which is embodied in UPP 2.4, an agency or organisation would be allowed a reasonable period within which to consider whether it can lawfully collect the unsolicited information, and whether it wishes to retain that information. If the collection is lawful and the agency or organisation decides to keep the information, the obligations that apply to the “active” collection of personal information should apply. If the collection is unlawful or the agency or organisation does not wish to retain the information, it should destroy the information as soon as practicable without using or disclosing it — if it is lawful and reasonable to do so.³⁵

2.53 The ALRC considered that use or disclosure for the purpose of determining whether the information should be retained would be

33. See ALRC Report 108 vol 1 [21.38].

34. ALRC Report 108 vol 1 Recommendation 21-3.

35. ALRC Report 108 vol 1 [21.55].

permissible under the recommendation. For example, an agency or organisation may need to use or disclose the information for the purpose of obtaining advice on whether to retain or destroy it.³⁶

2.54 The ALRC said that the above approach should prevent the expansion of the range of personal information that an agency or organisation may lawfully retain, use and disclose merely because it has taken no steps to collect the information. It emphasised that the requirement that an agency or organisation is only permitted to collect personal information that is “necessary for one or more of its functions or activities” would also apply to unsolicited personal information.³⁷

2.55 The ALRC acknowledged the concerns raised in some of the submissions regarding potential difficulties in complying with the obligations imposed by the privacy principles in respect of certain unsolicited information. Some submissions, for example, expressed concerns about complying with the notification principle, which imposes obligations on agencies and organisations to notify, or otherwise ensure, that an individual is aware of certain matters concerning the collection of his or her personal information. This is of particular relevance to agencies that accept and use unsolicited personal information through anonymous and confidential “tip-offs” that may be useful in investigations of offences and other unlawful activities.³⁸

2.56 The ALRC, however, emphasised that the requirement to comply with relevant privacy principles includes a consideration of any qualifications or exceptions to those principles. It noted, for example, that the obligation to notify, or otherwise ensure, that an individual is aware of certain matters concerning the collection of his or her personal information is limited to taking such steps, if any, that are reasonable in the circumstances. It expressed the view that, in some circumstances, it will be reasonable for an agency or organisation to take no steps to notify an individual about the collection of personal information, including the receipt of unsolicited confidential “tip-offs” relating to unlawful activity.³⁹

36. ALRC Report 108 vol 1 [21.55].

37. ALRC Report 108 vol 1 [21.56].

38. ALRC Report 108 vol 1 [21.47].

39. ALRC Report 108 vol 1 [21.54].

2.57 The ALRC also recommended that the OPC develop and publish guidance about the meaning of “unsolicited” in the context of the collection principle.⁴⁰

The law in NSW

2.58 Section 4(5) of PPIPA provides that for its purposes, “personal information is not collected by a public sector agency if the receipt of the information by the agency is unsolicited”.

2.59 Section 10 of HRIPA provides that, for its purposes, “health information is not collected by an organisation if the receipt of the information by the organisation is unsolicited.”⁴¹

2.60 Neither PPIPA nor HRIPA define the meaning of “collected” or “collection”. Nor do they specify which IPPs or HPPs, if any, apply to unsolicited personal information. Further, there is a lack of consensus on this matter among the cases decided by the NSW Administrative Decisions Tribunal (“the Tribunal”).⁴²

2.61 In *KD v Registrar, New South Wales Medical Board*, the Tribunal held that the personal information that KD included in her complaint lodged with the NSW Medical Board against a doctor was unsolicited.⁴³ The Tribunal ruled that s 8, 9, 10 and 11 of PPIPA, all of which relate to collection of personal information, had no application to unsolicited personal information.⁴⁴

2.62 The NSW Privacy Commissioner made a submission to the Tribunal arguing that the other IPPs in s 12-19 should be applied to

40. ALRC Report 108 vol 1 Recommendation 21-4.

41. *Health Records and Information Privacy Act 2002* (NSW) s 10.

42. See A Johnston, *PPIPA in Practice: An Annotated Guide to the Privacy and Personal Information Protection Act 1998 (NSW)*, [28].

43. KD wrote a letter to the NSW Health Minister complaining about a doctor who performed surgery on KD. The Minister forwarded KD’s letter to the Health Care Complaints Commission, which in turn referred KD’s letter to the NSW Medical Board. In the course of dealing with KD’s complaint against the doctor, the Board provided the doctor with documents that KD had given to the Board, including copies of correspondence and a Medicare claims history statement.

44. *KD v Registrar, NSW Medical Board* [2004] NSWADT 5 [28]. Compare *OA v New South Wales Department of Housing* [2005] NSWADT 233; *OA v New South Wales Department of Housing (No 2)* [2006] NSWADT 94, discussed below.

personal information *held* by agencies, irrespective of whether that information was collected. He submitted that once an agency “holds” personal information, s 12-19 come into play.⁴⁵ The Tribunal, however, held that, while s 19 (special restrictions on disclosure of personal information) catches all personal information held by an agency, s 17 (limits on the use of personal information)⁴⁶ and most of the provisions of s 18 (limits on disclosure of information) apply only to information that is “collected”, and accordingly do not apply to unsolicited information.⁴⁷

2.63 However, the Tribunal distinguished sub-section 18(1)(b), which unlike s 18(1)(a), does not refer to “collected information”.⁴⁸ The Tribunal held that s 18(1)(b) ought to be given wide interpretation to make it applicable to both collected and unsolicited personal information.

2.64 The decision in *KD v Registrar, NSW Medical Board* may be compared with other Tribunal decisions that have construed the term “collected” in s 4(5) of PPIPA and s 10 of the HRIPA broadly, thus enabling the application of the privacy principles to personal information that was not actively collected by agencies or organisations.

2.65 In *OA v New South Wales Department of Housing*,⁴⁹ the NSW Department of Housing (“the Department”) received information from

45. *KD v Registrar, New South Wales Medical Board* [2004] NSWADT 5 [28].

46. Compare *OA v New South Wales Department of Housing* [2005] NSWADT 233 and *AW v Vice Chancellor, University of Newcastle* [2008] NSWADT 86, where the Tribunal applied s 17 to personal information that was not actively solicited by the relevant agencies.

47. *KD v Registrar, NSW Medical Board* [2004] NSWADT 5 [29].

48. Section 18 (1) provides that a public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless: (a) 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, or (b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or (c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

49. *OA v New South Wales Department of Housing* [2005] NSWADT 233; *OA v New South Wales Department of Housing (No 2)* [2006] NSWADT 94.

members of the public alleging that OA, a public housing tenant, was sub-letting the unit provided to him by the Department while living elsewhere. Acting on this information, an officer of the Department interviewed OA about the allegations. OA denied the allegations and lodged with the Tribunal an application for review of the Department under PPIPA.

2.66 The Tribunal held that:

If the agency ... decides to “hold” information that was originally received as an unsolicited communication, then the principles in the Act that have to do with the “holding” of information come into play, as do the principles in relation to “use” and “disclosure” if action of that kind occurs.⁵⁰

2.67 The Tribunal applied s 16 of PPIPA, which by its terms, refers to the “holding” of personal information thus:

A public sector agency that holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

2.68 The Tribunal held that there was no breach of this section because the Department took reasonable steps to ensure the accuracy of the unsolicited information it received when one of its officers interviewed AO about the allegations.⁵¹

2.69 The Tribunal also applied s 17 of PPIPA, which provides:

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless:

- (a) the individual to whom the information relates has consented to the use of the information for that other purpose, or
- (b) the other purpose for which the information is used is directly related to the purpose for which the information was collected, or
- (c) the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health

50. *OA v New South Wales Department of Housing* [2005] NSWADT 233 [45].

51. *OA v New South Wales Department of Housing* [2005] NSWADT 233 [47]; *OA v New South Wales Department of Housing (No 2)* [2006] NSWADT 94 [21]-[26].

of the individual to whom the information relates or of another person.

2.70 The Tribunal held that “collection” occurred when the Department decided to retain the unsolicited information and keep it essentially as intelligence information. It went on to say that the personal information of AO was “collected” for investigative purposes and was also used for this purpose. Consequently, there was no breach of s 17.⁵²

2.71 In further contrast to the judgment in *KD v Registrar, NSW Medical Board*, the Tribunal in *OA v New South Wales Department of Housing* applied the collection principles in s 8 (collection of personal information for lawful purposes) and 9 (collection of personal information directly from individual) to personal information that was not actively solicited by the agency. It found, however, that there was insufficient evidence to support OA’s allegation that the Department breached s 8, and the Department’s Privacy Code of Conduct allowed it to depart from the provisions of s 9 when receiving complaints about the conduct of its tenants.⁵³

2.72 The case of *AW v Vice Chancellor, University of Newcastle*⁵⁴ also applied some privacy principles to unsolicited personal information. It involved a student (AW) who complained to the complaints manager of the University of Newcastle (“the university”), Ms Foster, about alleged harassment from fellow students and university staff. AW disclosed his HIV status in his complaint. Subsequently, AW lodged with the Tribunal an application for review of the conduct of the university, in particular the disclosure by Ms Foster of AW’s HIV status to other university officials, which was done in the course of the investigations relating to AW’s complaint.

2.73 The Tribunal examined whether the “use” by Ms Foster of AW’s personal information breached s 17 of the PPIPA and HPP 10 of the HRIPA, both of which prohibit the use of personal information for a purpose other than that for which it was collected, subject to certain exceptions. The Tribunal noted that these principles, by their terms, require that use be considered in the context of the purpose for which

52. *OA v New South Wales Department of Housing* [2005] NSWADT 233 [50].

53. *OA v New South Wales Department of Housing* [2005] NSWADT 233 [42]; *OA v New South Wales Department of Housing* (No 2) [2006] NSWADT 94 [17]-[20].

54. *AW v Vice Chancellor, University of Newcastle* [2008] NSWADT 86.

information was “collected”. It then construed the meaning of “collected” in the following manner:

While the information in this matter was not “collected” for the purposes of either section 10 of the Health Records Act or section 4(5) of the Privacy Act, decisions of the Tribunal have read the word “collected” in this context more broadly, to mean “obtained”.⁵⁵

2.74 The Tribunal held that the university did not breach the relevant privacy principles since AW’s primary purpose in providing the relevant personal information was so that Ms Foster could investigate his complaint, and Ms Foster’s use of that information when she discussed the applicant’s allegations with the university staff members concerned was use for that primary purpose.⁵⁶

Submissions

2.75 In CP 3, the Commission asked whether any or all of the IPPs and HPPs should apply to unsolicited personal information.⁵⁷

2.76 The Public Interest Advocacy Centre and the Australian Privacy Foundation both recommended that all of the IPPs and the HPPs should apply to all personal information, however obtained, to the maximum extent practicable in the circumstances.⁵⁸ The Public Interest Advocacy Centre said that the distinction between solicited and unsolicited personal information adds unnecessary complexity to the current law.⁵⁹

2.77 The NSW Law Society, the HIV/AIDS Legal Centre, and the Cyberspace Law and Policy Centre said that all the IPPs and HPPs should apply to unsolicited personal information except those in respect of collection.⁶⁰ The HIV/AIDS Legal Centre argued that:

where an organisation chooses to retain “unsolicited information”, and where that information continues to fall within “personal

55. *AW v Vice Chancellor, University of Newcastle* [2008] NSWADT 86 [28] citing *MT v Department of Education and Training* [2004] NSWADT 194.

56. *AW v Vice Chancellor, University of Newcastle* [2008] NSWADT 86 [29].

57. NSWLRC CP 3 Issue 23.

58. Public Interest Advocacy Centre, *Submission*, 15; Australian Privacy Foundation, *Submission*, 9.

59. Public Interest Advocacy Centre, *Submission*, 15.

60. The Law Society of NSW, *Submission*, 8; HIV/AIDS Legal Centre, *Submission*, 11; Cyberspace Law and Policy Centre, *Submission*, 14-15.

information”, it is difficult to ascertain policy reasons to exempt this information from any of the IPPs, barring possibly IPP 1 & 2 (information collected to be for a lawful purpose & directly relevant; information collected to be from individual directly).⁶¹

The Commission’s conclusions

2.78 As noted above, there is a lack of clarity under current legislation and case law about whether the IPPs and HPPs (and which, if any) apply to unsolicited personal information. There is a need for legislation to provide certainty and clarity on the matter. For this purpose, the Commission supports UPP 2.5, which outlines the options that agencies have in dealing with unsolicited information.

2.79 Under UPP 2.5, an agency is given a reasonable time within which to decide whether it can lawfully collect the unsolicited information, and whether it wishes to retain that information. If the agency decides to keep the information, it will have to comply with all relevant provisions in the privacy principles as if it had taken active steps to collect the information. If the agency decides not to retain the information, it will have to destroy the information as soon as practicable without using or disclosing it, if it is lawful and reasonable to do so. However, use or disclosure of the information for the purpose of determining whether the agency can and should retain it would be permissible, for example, where an agency seeks advice on whether to hold or destroy it.⁶²

2.80 As observed by the ALRC, the requirement in UPP 2.5 for agencies to comply with relevant privacy principles entails a consideration of any qualifications or exceptions to those principles. For example, the obligation to notify an individual of certain matters concerning the collection of his or her personal information (such as the fact of such collection, the purpose of collection, etc) is limited to taking such steps, *if any*, that are reasonable in the circumstances. Such limitation includes taking no steps, for example, where notification would defeat the purpose of the collection, such as where it would prejudice the enforcement of laws.⁶³

61. HIV/AIDS Legal Centre, *Submission*, 11.

62. ALRC Report 108 vol 1 [21.55].

63. See para 3.24-3.28.

SENSITIVE INFORMATION

2.81 This section examines UPP 2.5 and UPP 2.6, which have been formulated for the purpose of regulating the collection of sensitive information. These UPPs provide:

- 2.5 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:
- (a) the individual has consented;
 - (b) the collection is required or authorised by or under law;
 - (c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information concerns is legally or physically incapable of giving or communicating consent;
 - (d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual to whom the information concerns that the organisation will not disclose the information without the individual's consent;
 - (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;
 - (f) the collection is necessary for research and all of the following conditions are met:
 - (i) the purpose cannot be served by the collection of information that does not identify the individual or from which the individual would not be reasonably identifiable;
 - (ii) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection;
 - (iii) a Human Research Ethics Committee that is constituted in accordance with, and acting in

compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act; and

- (iv) the information is collected in accordance with Research Rules issued by the Privacy Commissioner; or
- (g) the collection is necessary for the purpose of a confidential alternative dispute resolution process.

2.6 Where an agency or organisation collects sensitive information about an individual in accordance with 2.5(f), it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Current law

Commonwealth

2.82 Section 6(1) of the Privacy Act defines sensitive information as information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices;
- criminal record;
- health information; or
- genetic information that is not otherwise health information.

2.83 This definition is relevant for purposes of NPP 10.1, which provides:

- 10.1 An organisation must not collect sensitive information about an individual unless:
- (a) the individual has consented; or
 - (b) the collection is required by law; or
 - (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
 - (i) is physically or legally incapable of giving consent to the collection; or
 - (ii) physically cannot communicate consent to the collection; or
 - (d) if the information is collected in the course of the activities of a non-profit organisation — the following conditions are satisfied:
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or
 - (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

2.84 By restricting the circumstances when sensitive information may be collected, NPP 10.1 provides sensitive information with a higher level of protection than other forms of personal information. However, these restrictions apply only to organisations. There are no counterpart provisions in the Principles and consequently, agencies covered by the Privacy Act are not under similar restrictions when collecting sensitive information.

NSW

2.85 In NSW, PPIPA does not define sensitive information. Nevertheless, s 19 of PPIPA refers to “an individual's ethnic or racial

origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities”. These are similar to some of the information identified in s 6(1) of the Privacy Act as being sensitive information.

2.86 In contrast to NPP 10.1 (which regulates the collection of sensitive information by organisations) s 19 of PPIPA puts restrictions on *disclosure* of the categories of personal information it covers.⁶⁴ There are no other provisions in PPIPA that provide special rules relating to the collection of the categories of personal information enumerated in s 19.

2.87 HRIPA does not contain any provision that is comparable to NPP10.1 or s 19 of PPIPA.

Regulating the collection of sensitive information

2.88 The ALRC examined whether agencies covered by the Privacy Act should also be subject to restrictions in collecting sensitive information, and if so, where such restrictions should be located.

2.89 The ALRC recommended that the UPPs should set out requirements that both agencies and organisations must observe when collecting personal information that is defined as sensitive information for the purposes of the Privacy Act. Further, its recommendation stated that the relevant requirements should be located in the collection principle.⁶⁵

2.90 The ALRC declared that there are strong policy reasons for regulating the collection of sensitive information by both agencies and organisations. It said that the categories of personal information that are defined as sensitive information need to be given a higher level of protection than other forms of personal information because they are highly personal in nature and their misuse can be quite damaging to the individual concerned. They can, for example, be used as a basis for unjustified discrimination and other forms of mistreatment.⁶⁶

2.91 With respect to the location of the provisions on the collection of all sensitive information, the ALRC argued that it would be inappropriate to regulate the collection of sensitive information in a separate principle

64. Disclosure of sensitive information is dealt with in para 5.48-5.54.

65. ALRC Report 108 vol 1 Recommendation 22-1.

66. ALRC Report 108 vol 1 [22.19]-[22.21].

because it may “convey the incorrect impression that there is a completely separate regime applicable to sensitive information at all stages of the information cycle”.⁶⁷ As a general rule, the UPPs apply to all personal information, including sensitive information. However, there are specific provisions for sensitive information, such as those relating to collection, use and disclosure,⁶⁸ and direct marketing.⁶⁹

2.92 The Commission supports the ALRC’s recommendation. It agrees with the view expressed by the ALRC that the categories of personal information defined under the Privacy Act as sensitive information deserve a greater level of protection than other forms of personal information because they are highly personal in nature and the individuals to whom they relate would generally have a reasonable expectation that they should remain private. The recommendation by the ALRC to regulate the collection of sensitive information through specific provisions in the collection principle is of particular significance to NSW because, as indicated above, PPIPA and HRIPA do not currently have provisions regulating the collection of sensitive information. The Commission considers it critical that the protection given to sensitive information should commence from the collection stage.

Prohibiting collection as the starting point

2.93 The ALRC used NPP 10.1 as the main basis for its regulatory approach to the collection of sensitive information, which involves prohibition as the starting point subject to well-defined exceptions. The following sections examine the specific circumstances when sensitive information may be collected pursuant to UPP 2.5.

Consent

2.94 UPP 2.5(a) allows the collection of sensitive information where the individual to whom the information relates has consented.

2.95 This is similarly worded to NPP 10.1(a). There was a suggestion from privacy advocates that UPP 2.5(a) should, as an improvement on NPP 10.1(a), require express consent.⁷⁰ However, the ALRC took the position that a requirement of express consent would be impracticable

67. ALRC Report 108 vol 1 [22.22]-[22.23].

68. See para 5.10.

69. See para 6.13.

70. ALRC Report 108 vol 1 [22.65].

and too prescriptive, particularly in relation to health information.⁷¹ It noted that the OPC's *Guidelines on Privacy in the Private Health Sector* recognise that there are situations where it is reasonable for health service providers to rely on the implied consent of patients. The pertinent provisions of these *Guidelines* provide:

As a general rule, if a health service provider needs or wants consent and is in doubt about whether an individual is giving consent or not, it is preferable to seek express consent.

Implied consent – there are situations when health service providers may reasonably rely on implied consent by individuals to handle health information in certain ways.

For example, an individual presents to a medical practitioner, discloses health information, and this is written down by the practitioner during the consultation – this will generally be regarded as giving implied consent to the practitioner to collect the information for certain purposes. The extent of these purposes will usually be evident from the discussion during the consultation.

Similarly, if a medical practitioner collects a specimen to send to a pathology laboratory for testing, it would be reasonable to consider that the individual is giving implied consent to the passing of necessary information to that laboratory.

Where there is open communication and information sharing between the health service provider and the individual, consent issues will usually be addressed during the course of the consultation. If the discussion has provided the individual with an understanding about how their health information may be used, then it would be reasonable for the health service provider to rely on implied consent.⁷²

2.96 The Commission supports the ALRC's position that collectors of sensitive information should be able to rely on the express or implied consent of the individual concerned. Quite often, reliance on the consent is a matter of convenience for both the collector and the individual concerned.

2.97 The Commission agrees with the ALRC that collectors of sensitive information should be able to rely on the implied consent of the

71. ALRC Report 108 vol 1 [22.22]-[22.23].

72. Office of the Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001) A.5.3.

individual concerned. The OPC guidelines quoted above give illustrations of circumstances where it would be more practicable for both medical health practitioners and patients if reliance can be had on implied consent. The guidelines also underscore the preferred approach of seeking express consent when in doubt whether or not the individual is giving consent. Finally, they indicate that, at least with respect to health information, the implied consent must also be the result of an informed decision.

2.98 Attention should be drawn to the ALRC's recommendation that the OPC develop and publish guidance on consent that addresses express and implied consent as it applies in various contexts.⁷³ The Commission agrees with the ALRC's contention that guidance from the OPC provides a more flexible mechanism for dealing with this issue,⁷⁴ and endorses the adoption of such an approach in NSW. It considers the provisions on implied consent in the OPC's *Guidelines on Privacy in the Private Health Sector* to be a good model that could be expanded to cover situations relating to sensitive information other than health information. The guidelines should, however, make it clear that a collector of sensitive information should endeavour to obtain express consent whenever practicable before relying on implied consent.

Collection is required or authorised by or under law

2.99 UPP 2.5(b) allows the collection of sensitive information where this is required or authorised by or under law.

2.100 This provision may be compared with NPP 10.1(b), which allows the collection of sensitive information where it is required by law. The ALRC considered the provision in NPP 10.1(b) to be too narrow because it ostensibly does not allow the collection of sensitive information when authorised by law. The ALRC said that the wording of UPP 2.5(b) is particularly relevant to agencies that are authorised by law to collect sensitive information as a means of assisting them perform their statutory functions, such as those relating to law enforcement and the administration of government programs.⁷⁵

2.101 The ALRC also said that the collection of sensitive information need not be *specifically* authorised by law. It made the observation that

73. ALRC Report No 108 (2008) vol 1 Recommendation 19-1.

74. ALRC Report 108 vol 1 [22.70].

75. ALRC Report 108 vol 1 [22.31].

information-gathering powers of agencies do not usually refer specifically to sensitive information. Consequently, in its view, an exception that permits the collection of sensitive information only where it is specifically authorised by or under law would be too restrictive.⁷⁶

2.102 The Commission supports UPP 2.5(b) and does not have anything to add to the ALRC’s reasons and commentary.

Emergency situations

2.103 UPP 2.3(c) allows the collection of sensitive information where it is necessary to prevent or lessen a serious threat to the life or health of any individual, and where the individual to whom the information relates is legally or physically incapable of giving or communicating consent.

2.104 The current requirement under NPP 10.1(c) requires the threat to the life or health of any individual to be both serious and imminent. The ALRC considered such a requirement to be too difficult to satisfy and decided that it should be relaxed so that the exception in UPP2.3(c) could be used where a threat is serious, but not necessarily imminent. It said that this would enable an agency or organisation to take preventative action to avert a threat from becoming a full-blown crisis. Further, it said that the formulation in UPP 2.3(c) strikes an appropriate balance between protecting the privacy rights of an individual and the public interest in preventing threats to life and health.⁷⁷

2.105 One submission to the ALRC suggested replacing the word “imminent” with another qualification that suggests likelihood, such as “probable” or “likely”. The ALRC decided that this was unnecessary because in its view, “[i]f it is improbable that a threat will eventuate, then the threat cannot be considered serious”.⁷⁸

2.106 The Commission agrees with the ALRC that it should be enough for a threat to be serious to justify the collection of sensitive information. A threat may not be imminent but may be of a level of seriousness that a public interest exists in collecting sensitive information. An example might be where an animal disease has infected a small number of people, some of whom have died, in a few countries. There are concerns among health authorities that the disease has a potential to become a human

76. ALRC Report 108 vol 1 [22.32].

77. ALRC Report 108 vol 1 [22.48].

78. ALRC Report 108 vol 1 [22.49].

pandemic but it has so far been confined to a few specified countries and has not yet been documented in Australia. It has not yet been included in the list of notifiable diseases in relevant legislation⁷⁹ and is therefore not covered by the provision in UPP 2.5(b) allowing the collection of sensitive information where it is required by law. Because the disease in question may have a lengthy incubation period, has not yet reached Australia, and there is a chance that it could be contained in the few countries where it has been detected, it might be argued that, although it is a serious threat, it is not yet an imminent threat to Australia. However, its potential to reach Australia and become a pandemic arguably poses a serious threat to the health of a large number of individuals. This should be sufficient to justify the collection of relevant health information (for example, screening the health of individuals who have recently travelled to countries where the condition has been detected and who have certain symptoms) to enable authorities to monitor the situation, take steps to prevent a health crisis from happening, and formulate a management plan in case the disease reaches Australia.

2.107 The Commission also agrees with the position taken by the ALRC that it is unnecessary to specify that the serious threat should also be “probable” or “likely”. The determination of the seriousness of a threat will usually involve an assessment of the probability of it happening.

Non-profit organisations

2.108 UPP 2.5(d) allows the collection of sensitive information if the information is collected in the course of the activities of a non-profit organisation and the following conditions are present:

- the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and
- at or before the time of collecting the information, the organisation undertakes to the individual to whom the information concerns that the organisation will not disclose the information without the individual’s consent.

2.109 UPP 2.5(d) mirrors the wording of NPP 10.1(d). There was very little discussion on UPP 2.5(d) in the ALRC Report, which may have been due to scant feedback on the matter from the submissions.

79. See *Public Health Act 1991* (NSW).

2.110 There was one suggestion from the submissions that this exception be redrafted to allow the collection of sensitive information “if the information is collected in the course of the lawful activities of a non-profit organisation *that has aims relating to sensitive information (as defined in the [Privacy] Act)*”.⁸⁰ The ALRC said that concerns about the drafting of this exception will best be addressed by the OPC.⁸¹

2.111 The ALRC also said that the definition of “non-profit organisation” should not be located in the collection principle but should be situated in Pt II of the Privacy Act, which deals with interpretation of terms.⁸² Currently, the definition of this term is found in the principle dealing with sensitive information.⁸³ The ALRC argued that it is logical to locate the definition of this term with the other definitions in the Privacy Act. Further, it said that this approach would simplify the provisions of the collection principle relating to sensitive information.⁸⁴

2.112 The Commission supports UPP 2.5(d) and does not have further comments or suggestions. We note that this particular exception will not have relevance in NSW since PPIPA does not cover organisations.

Legal and equitable claims

2.113 UPP 2.5(e) allows the collection of sensitive information where it is necessary for the establishment, exercise or defence of a legal or equitable claim.

2.114 This is based on, and similarly worded to, NPP 10.1(e). The ALRC did not recommend any changes to the wording of NPP 10.1(e). It said that it “did not receive sufficient feedback from stakeholders to enable it to assess properly the merits and consequences of broadening the exception”.

2.115 The Commission supports UPP 2.5(e).

Research

2.116 There is no provision in NPP 10.1 allowing the collection of sensitive information for research purposes. However, NPP 10.3 allows organisations to collect health information (which is a category of

80. ALRC Report 108 vol 1 [22.67], emphasis added.

81. ALRC Report 108 vol 1 [22.71].

82. ALRC Report 108 vol 1 [22.72].

83. *Privacy Act 1988* (Cth) sch 3 NPP 10.5.

84. ALRC Report 108 vol 1 [22.72].

sensitive information) without the consent of the individual concerned where the collection is necessary for purposes of research, or the compilation or analysis of statistics⁸⁵ and the following conditions are present:

- it is relevant to public health or safety;
- the purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained;
- it is impracticable for the organisation to seek the individual's consent to the collection; and
- the information is collected as required by law; or in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or in accordance with guidelines issued by the National Health and Medical Research Council ("NHMRC") and approved by the OPC under s 95A of the Privacy Act.

2.117 Further, NPP 10.4 provides that, if an organisation collects health information about an individual in accordance with NPP 10.3, the organisation must take reasonable steps permanently to de-identify the information before the organisation discloses it.

2.118 The ALRC recommended the expansion of the research exception beyond health and medical research to apply to human research generally. It reasoned that other areas of research, such as sociology and criminology, should be supported because of their potential to lead to evidence-based policy that could benefit the community. Further, it argued that research is increasingly becoming multi-disciplinary and that non-health information is often desirable or necessary in some health and medical research.⁸⁶

2.119 The ALRC used NPP 10.3 and NPP 10.4 as the basis for UPP 2.5(f) and UPP 2.6, which are the model privacy principles on the collection of sensitive information for the purpose of research.

2.120 UPP 2.5(f) allows the collection of sensitive information for the purpose of research if all these conditions are met:

85. A third purpose covered by NPP 10.3 is the management, funding, or monitoring of a health service.

86. ALRC Report 108 vol 3 [65.40].

- the purpose cannot be served by the collection of information that does not identify the individual, or from which the individual would not be reasonably identifiable;
- it would be unreasonable or impracticable for the agency or organisation to seek the individual’s consent to the collection;
- a Human Research Ethics Committee (“HREC”) that is constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act; and
- the information is collected in accordance with research rules issued by the OPC.

2.121 There are three main changes to the current requirements. The first relates to the “unreasonable or impracticable” requirement. Currently, NPP 10.3 allows the collection of health information for research without consent where it is *impracticable* for the organisation to seek the individual’s consent before the collection, use or disclosure. The ALRC, in response to submissions, acknowledged that the impracticable requirement “may not be the clearest and most appropriate test in some circumstances”. It explained that it might be practicable to get the consent from individuals to collect and use their personal information for the purposes of research in the sense that it is logistically possible, but obtaining such consent may have an adverse impact on the integrity and validity of the research. It gave the view that the term “impracticable” relates more to the process of obtaining consent rather than to the impact of obtaining consent.⁸⁷

2.122 It noted that the guidelines that the NHMRC may issue under s 95 of the Privacy Act for the protection of privacy in the conduct of medical research contain a reasonableness test; that is, research may proceed without consent when it is reasonable to do so. The ALRC gave the view that “[w]hile it might be practicable to seek the consent of research participants in a particular case, it would not be reasonable to do so if this would have an unacceptable impact on the integrity and validity of the research”. It concluded that both the reasonable and impracticable tests

87. ALRC Report 108 vol 3 [65.94].

should be incorporated in UPP 2.5.⁸⁸ Hence, one of the requirements for the collection of sensitive information under UPP 2.5 is that it would be unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection.

2.123 The second change relates to the new requirement for a public interest review by HRECs. This embodies the ALRC's view about the need to balance the public interest in the proposed research and the interest in protecting the privacy of individuals subject of the research. It said that:

If, taking all relevant factors into account, the public interest in one course of action outweighs the public interest in another course of action, the appropriate course of action is clear. In particular — in the research environment where a range of other safeguards are in place — if the public interest in a particular research proposal going forward outweighs the public interest in maintaining the level of privacy protection provided by the privacy principles, then the research should be allowed to proceed.⁸⁹

2.124 The ALRC decided that the determination of whether the public interest in the proposed research outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act should be made by HRECs.⁹⁰ In Australia, HRECs are one of the main means for ensuring the ethical design, review and conduct of human research. The HREC required under UPP 2.5(f)(iii) must be constituted in accordance with the *National Statement on Ethical Conduct in Human Research* (2007), which was jointly developed by the NHMRC, the Australian Research Council and the Australian Vice-Chancellors' Committee for the purpose of, among other things, providing guidelines to HRECs on conducting ethical review of research.

2.125 The third change is the provision that the sensitive information must be collected in accordance with research rules issued by the OPC. In contrast to this provision, the current provision states that the health information may be collected if, in addition to the other requirements:

- the information is collected as required by law;

88. ALRC Report 108 vol 3 [65.95]-[65.96].

89. ALRC Report 108 vol 3 [65.81].

90. ALRC Report 108 vol 3 Recommendation 65-4.

- it is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality that bind the organisation; or
- it is collected in accordance with guidelines issued by the NHMRC and approved by the OPC approved under s 95A of the *Privacy Act*.

2.126 The ALRC decided that the first of these three alternative requirements is unnecessary because the collection principle (in UPP 2.5(b)) already provides that the collection of sensitive information without consent is allowed where the collection is required or authorised by or under law.⁹¹

2.127 The ALRC decided to dispense with the second alternative requirement because it has never been used.⁹²

2.128 The ALRC recommended the revision of the third alternative requirement so that the collection must now be in accordance with research rules issued by the OPC.

2.129 The first thing to note about the revised requirement is the use of the term “rules” instead of “guidelines”. This is to underline the fact that the research rules to be issued by the OPC will be binding.⁹³

2.130 The ALRC said that, since the research exception to collection of sensitive information is being broadened to cover all human research and not just health and medical research, it would no longer be appropriate for the NHMRC to issue the research rules.⁹⁴

2.131 Further, it said that the research exceptions to collection and use of sensitive information would have the effect of allowing the use of such personal information in ways that would normally breach the UPPs. It argued that, in this respect, the research rules issued under those exceptions are similar in effect to Public Interest Determinations, which are made by the OPC pursuant to its powers under the *Privacy Act*.⁹⁵ It

91. ALRC Report 108 vol 3 [65.157].

92. The OPC informed the ALRC that it is not aware of rules established by competent health or medical bodies that would fulfil the requirements of NPP 10.3: ALRC Report 108 vol 3 [65.157].

93. ALRC Report 108 vol 3 [65.5]-[65.6].

94. ALRC Report 108 vol 3 [65.19].

95. *Privacy Act 1988* (Cth) s 72.

said that the OPC's involvement is required where there are changes to the level of protection provided by the UPPs.⁹⁶

2.132 With respect to the requirement in NPP 10.4, the ALRC recommended that its wording be modified so that an agency or organisation that collected sensitive information under the research exception should no longer be required to take reasonable steps to "permanently de-identify" information before it is disclosed. Instead, under UPP 2.6, where an agency or organisation collects sensitive information about an individual in accordance with the research exception, it must "take reasonable steps to ensure that the information is not disclosed in a form that would identify individuals or from which individuals would be reasonably identifiable".

2.133 The ALRC argued that the new provision is more consistent with its recommended definition of personal information,⁹⁷ which is "information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual".⁹⁸

2.134 Reasonable steps under UPP 2.6 would include employing commonly-used research techniques that are intended to protect confidentiality, such as "data suppression" where certain research data, such as the personal information of research subjects, are kept under wraps.⁹⁹

2.135 The Commission supports UPP 2.5(f) and UPP 2.6 and has no comments or suggestions.

Alternative dispute resolution

2.136 UPP 2.5(g) allows the collection of sensitive information where it is necessary for the purpose of a confidential alternative dispute resolution ("ADR") process.

2.137 This is a new provision that the ALRC recommended in recognition of the critical role of alternative dispute resolution in the effective, efficient and fair resolution of disputes. The ALRC also acknowledged that disclosure of all relevant information by the parties to

96. ALRC Report 108 vol 3 [65.17].

97. ALRC Report 108 vol 3 [65.160].

98. ALRC Report 108 vol 1 Recommendation 6-1.

99. ALRC Report 108 vol 3 [65.163].

an ADR process, including sensitive information about themselves and relevant third parties, is an important aspect of ADR processes.¹⁰⁰

2.138 The National Alternative Dispute Resolution Advisory Council (NADRAC), in its submission to the ALRC, underscored the significance of information sharing by the parties to ADR processes. The NADRAC commented that:

ADR processes are aimed at getting each party to outline the full context of the dispute from their perspectives with a view to identifying the underlying interests of each party ... In the course of 'telling their story' many parties will include information that seems to them to be important and which may help to indicate how they came to their position but which would be deemed irrelevant in legal proceedings. The accounts will often include personal information including sensitive information about themselves and others whom the person considers to be directly or indirectly involved.¹⁰¹

2.139 The ALRC also acknowledged that, unless certain exceptions are adopted relating to ADR, the Privacy Act has the potential to prevent disclosure of information in the context of ADR. For example, the collection principle may prevent agencies and organisations that provide ADR services from receiving sensitive personal information about third parties where they do not have that person's consent. Further, the use and disclosure principle may prevent those agencies and organisations from using or disclosing sensitive personal information that relates to a party to the dispute if that person withholds consent, for example, where the information could undermine that party's position.¹⁰²

2.140 The ALRC therefore recommended that agencies and organisations be permitted to collect sensitive information under the collection principle, and to use and disclose personal information under the use and disclosure principle, where the collection, use or disclosure is necessary for the purpose of an ADR proceeding.¹⁰³

100. ALRC Report 108 vol 2 [44.23]-[44.24].

101. ALRC Report 108 vol 2 [44.6].

102. ALRC Report 108 vol 2 [44.25].

103. ALRC Report 108 vol 2 Recommendation 44-1. The aspect of this recommendation relating to the use and disclosure principle is discussed in Chapter 5.

2.141 UPP 2.5(g) contains a qualification that the relevant ADR proceeding must be confidential in nature. The ALRC considered that the confidentiality requirements attached to ADR processes are the best way of safeguarding personal information collected through the recommended ADR exception. It gave the view that, provided the parties to the dispute and the ADR provider are bound by legal or contractual confidentiality obligations, any personal information that is collected pursuant to UPP 2.5(g) will be adequately protected, since its use or disclosure will be restricted to the particular ADR proceeding in which it was collected, unless the parties consent to its use or disclosure for other purposes, or another relevant exception applies.¹⁰⁴

2.142 The ALRC said that the OPC should, in consultation with NADRAC, formulate guidance on what constitutes confidentiality requirements for purposes of UPP 2.5(g).¹⁰⁵

2.143 The ALRC decided that it is unnecessary to add a requirement that agencies or organisations providing ADR must be “authorised”, in the sense of being accredited through existing accreditation systems,¹⁰⁶ or through an accreditation system to be established specifically for purposes of the Privacy Act. It considers ADR to be “dynamic and diverse” and concluded that, provided confidentiality safeguards are in place, such diversity should be accommodated.¹⁰⁷

2.144 The Commission agrees with the ALRC’s view that ADR has become an essential element in the resolution of disputes in Australian society. ADR processes have become integrated with the judicial system, for example, through the power of courts to refer proceedings before it for mediation,¹⁰⁸ or through commercial arbitration legislation that confers power on courts that are supportive of the administration of the arbitration process.¹⁰⁹

104. ALRC Report 108 vol 2 [44.29]-[44.30].

105. ALRC Report 108 vol 2 [44.31].

106. For example, see para 2.146 and accompanying notes.

107. ALRC Report 108 vol 2 [44.33].

108. See, for example, *Uniform Procedure Act 2005* (NSW) pt 4.

109. *Commercial Arbitration Act 1984* (NSW).

2.145 In NSW, it is government policy for agencies to attempt, where possible, to settle disputes by using ADR techniques rather than by resorting to the court system.¹¹⁰

2.146 ADR processes have also become a common feature in resolving disputes involving private industries. For example, banks, credit unions, building societies and other entities that provide financial services to retail clients are required by law to be members of a dispute resolution scheme approved by the Australian Securities and Investments Commission¹¹¹ and this has resulted in the establishment and regulation of industry-funded ADR schemes,¹¹² which are intended to provide accessible justice for consumers.

2.147 An essential component of ADR techniques is the ability of parties to freely and candidly narrate their side of the dispute, which may involve giving sensitive information about themselves and others who may be involved with the dispute. The Commission supports UPP 2.5(g) since it would promote the free flow of information among parties to an ADR process and enable the ADR provider to receive sensitive information that may be required for the effective resolution of the dispute. The confidentiality requirements that are usually an essential aspect of the ADR processes and which are required for the operation of UPP 2.5(g) provide sufficient protection for any sensitive information collected in that context.

110. NSW Department of Premier and Cabinet Memorandum No 97-26 (1997). See also the *Model Litigant Policy* (2004) (it declares that the State and its agencies must act as a model litigant in the conduct of litigation, which means, among other things, using ADR whenever possible). For a recent NSW government initiative to promote the greater use of ADR, see NSW Attorney General's Department, *ADR Blueprint: Framework for the Delivery of Alternative Dispute Resolution (ADR) Services in NSW* (2009).

111. *Corporations Act 2001* (Cth) s 912(2)(b).

112. Examples of ASIC-approved dispute resolution schemes include the Banking and Financial Services Ombudsman, the Credit Union Dispute Resolution Centre, and the Financial Co-operative Dispute Resolution Scheme.

3. UPP 3: Notification

- Introduction
- A separate principle
- Nature and timing
- Exemptions
- Collection of personal information from a third party
- Content of notification

INTRODUCTION

3.1 This chapter examines the obligations of agencies and organisations to take steps to ensure that individuals are aware of certain matters when their personal information is being, or has been, collected. The Commission follows the lead of the ALRC in referring to these obligations as relating to “notification”, even though notification is only one way of achieving awareness.¹

3.2 In particular, the chapter analyses UPP 3, which the ALRC recommended as the reform model for the notification principle of the privacy legislation of each of the Australian jurisdictions. UPP 3 provides:

UPP 3. Notification

At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of, the:

- (a) fact and circumstances of collection, where the individual may not be aware that his or her personal information has been collected;
- (b) identity and contact details of the agency or organisation;
- (c) rights of access to, and correction of, personal information provided by these principles;
- (d) purposes for which the information is collected;
- (e) main consequences of not providing the information;
- (f) actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information of the kind collected;
- (g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency’s or organisation’s Privacy Policy; and

1. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) vol 1 [23.1].

- (h) fact, where applicable, that the collection is required or authorised by or under law.

3.3 The main issues relate to:

- whether the notification requirements should be contained in a separate privacy principle;
- the nature and timing of, and exemptions from compliance with, the notification requirements; and
- the matters that should be brought to an individual's awareness when his or her personal information is collected.

A SEPARATE PRINCIPLE

3.4 At the moment, the requirements relating to notification under the Privacy Act are located in Principle 2 and NPP 1.3. Both of these principles deal with the collection of personal information.

3.5 The ALRC in Report 108 recommended that:

The model Unified Privacy Principles should contain a principle called 'Notification' that sets out the requirements on agencies and organisations to notify individuals or otherwise ensure they are aware of particular matters relating to the collection and handling of personal information about the individual.²

3.6 The ALRC reasoned that dealing with notification in a separate principle recognises its importance in the information cycle, in particular, its role in encouraging transparency about an entity's collection and handling of personal information, as well as in informing individuals about the treatment of their personal information, and their rights in this regard.³

3.7 In NSW, the notification requirements are also found in principles relating to collection, namely:

- s 10 of PPIPA;⁴ and

2. ALRC Report 108 vol 1 Recommendation 23-1.

3. ALRC Report 108 vol 1 [23.13].

4. For illustration of an application of this section, see *SW v Forests NSW* [2006] NSWADT 74 (one of employees of Forests NSW took photographs of SW at a work-related function and did not take reasonable steps to ensure SW was aware that her photographs were being taken and the purpose for this).

- HPP 4 of HRIPA.

3.8 The Commission agrees with the ALRC’s recommendation that there should be a distinct principle called “notification” that spells out the obligations of agencies to notify individuals, or to otherwise ensure they are aware, of certain matters relating to the collection and handling of their personal information. Placing the notification requirements within a principle that regulates the *collection* of personal information does not give sufficient recognition to the importance of the notification requirements.

NATURE AND TIMING

3.9 At the Commonwealth level, agencies are required by Principle 2 to take such steps as are, in the circumstances, reasonable to ensure that an individual is aware of specified matters before it collects personal information or, if that is not practicable, as soon as practicable after the information is collected.⁵

3.10 Similarly, organisations are obligated by NPP 1.3 to take reasonable steps at or before the time of collection or, if that is not practicable, as soon as practicable after collection, to ensure that the individual concerned is aware of certain matters.⁶

Notification as a means of ensuring awareness

3.11 Principle 2 and NPP 1.3 do not refer specifically to an obligation to notify. The obligation under these principles is to take steps to ensure that an individual is aware of specified matters. The issue that arises is whether the notification principle should also refer to an obligation to notify as a means of ensuring awareness.

3.12 The ALRC recommended that the notification principle should expressly refer to notification as a means of ensuring that an individual is aware of specified matters relating to the collection of his or her personal information.⁷

3.13 It emphasised, however, that agencies and organisations should be able to rely on means other than notification to ensure that an individual

5. *Privacy Act 1988* (Cth) s 14 Principle 2.

6. *Privacy Act 1988* (Cth) sch 3 NPP 1.3.

7. ALRC Report 108 vol 1 [23.27], Recommendation 23-2.

is aware of specified matters. It observed that to require notification in every case would increase unnecessarily the compliance costs and may overload individuals with information of which they are already aware.⁸

3.14 It said that, as an example, a collecting agency or organisation could make inquiries or otherwise satisfy itself that an individual has been made aware of the specified matters by the agency or organisation which disclosed the information to it.⁹

3.15 Further, it said that it might be legitimate in some situations for agencies and organisations to alert the individual to specific sections of its Privacy Policy or other general documents as a means of ensuring that individuals are aware of the specified matters subject of the notification principle.¹⁰

3.16 In NSW, s 10 of PPIPA and HPP 4 are worded similarly to their counterpart Commonwealth principles in that they refer to an obligation to take reasonable steps to ensure that the individual whose personal information has been collected has been made aware of specified matters. They do not expressly refer to notification as a means of ensuring awareness.

3.17 The Commission is of the view that entities that collect personal information can comply with the obligation under s 10 of PPIPA and HPP 4 (as well as under Principle 2 and NPP 1.3) by giving notice to the individual concerned, for example, by written correspondence. They can also comply with the obligation through mechanisms other than a formal notice. For example, where personal information is collected through an online order form, the information that the agency is required to give to the individual under the notification principle can be displayed in the vicinity of the “submit” button that the individual clicks to send his or her personal information. Alternatively, where the agency’s Privacy Policy contains the specified matters required under the notification

8. ALRC Report 108 vol 1 [23.28].

9. ALRC Report 108 vol 1 [23.29].

10. ALRC Report 108 vol 1 [23.30]. The ALRC recommended that the OPC develop and publish guidance on the circumstances in which an agency or organisation can comply with specific requirements under the notification principle by alerting an individual to specific sections of its Privacy Policy or other general documents containing the requisite information: ALRC Report 108 vol 1 [23.31], Recommendation 23-3(c).

principle and the Privacy Policy is displayed prominently in the agency’s website, the individual may be required to acknowledge, prior to clicking the “submit” button, that he or she has read the Privacy Policy.¹¹

3.18 Although the Commission is of the view that the current provisions under both NSW and Commonwealth law already cover notification as a means of ensuring awareness of those matters that are the subject of the notification obligations, it nevertheless supports the ALRC recommendation. The provision in UPP 3 that those who collect personal information “must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of” certain matters clarifies that there may be several means of ensuring awareness and that notification is one of them.

Timing

3.19 In terms of timing, Principle 2 requires agencies to comply with the obligation before the collection of the personal information or, if that is not practicable, as soon as possible after the collection.¹² NPP 1.3 covers both time frames but also allows organisations to comply with the obligation at the time of the collection.¹³

3.20 The ALRC recommended that the timeframe for compliance with the requirements under the notification principle should be standardised pursuant to the aim of achieving uniform privacy principles for agencies and organisations. It used NPP 1.3 as its template for this purpose. Consequently, it recommended that the obligations under UPP 3 should be complied with before or at the time an agency or organisation collects personal information or, if that is not practicable, as soon as practicable thereafter.¹⁴

3.21 In NSW, s 10 of PPIPA identifies two timeframes for compliance: before the information is collected, or as soon as practicable after collection. Unlike UPP 3, it does not mention compliance at the time of collection, although this is implied. More importantly, compliance after

11. See J Douglas-Stewart, *Annotated Privacy Principles* (Adelaide, Presidian Legal Publications, 3rd ed, 2007) [2-360].

12. *Privacy Act 1988* (Cth) s 14 Principle 2.

13. *Privacy Act 1988* (Cth) sch 3 NPP 1.3.

14. ALRC Report 108 vol 1 [23.32], Recommendation 23-2.

collection under s 10 is not subject to the condition found in UPP 3 that compliance before or at the time of collection is not practicable.

3.22 In contrast to s 10, HPP 4 already reflects the timeframes specified in UPP 3.

3.23 The Commission supports the timeframes found in UPP 3. The wording in UPP 3 that compliance be “[a]t or before the time (or, if that is not practicable, as soon as practicable after)” of the collection of personal information is better than the provision in s 10 of PPIPA since it specifies the intent that agencies and organisations must endeavour to comply with the notification requirements before, or at, the time of collecting personal information, if this is practicable under the circumstances. It is crucial that collectors of personal information comply with the notification requirements at the earliest possible time to enable the individual concerned to make informed decisions about his or his personal information. However, UPP 3 also recognises that this may not be practicable in every situation.¹⁵

Reasonable steps include no steps

3.24 Currently, Principle 2 requires agencies to “take such steps (if any) as are, in the circumstances, reasonable” to ensure that the individual concerned is generally aware of specified matters. The phrase “if any” indicates that it might be reasonable for agencies to take no steps to provide notice under certain circumstances.

3.25 The phrase “if any” is absent in NPP 1.3, which requires organisations to “take reasonable steps to ensure that the individual is aware” of certain specified matters. As a consequence, the ALRC believes that there is uncertainty over whether organisations are able to determine that, in certain circumstances, it would be reasonable to take no steps.

3.26 The ALRC recommended that the UPP 3 should provide expressly that an agency or organisation is obliged to take “such steps, if any, as are reasonable in the circumstances” to notify or otherwise ensure that an individual is aware of specified matters.¹⁶

3.27 The ALRC said that this addresses the confusion caused by the use of the phrase “must take reasonable steps” in NPP 1.3, which, in its view,

15. See ALRC Report 108 vol 1 [23.33]-[23.34].

16. ALRC Report 108 vol 1 [23.48], Recommendation 23-2.

implies that organisations must always take some active steps to comply with the notification obligations. The ALRC asserted that “in certain circumstances, logic dictates that it would be reasonable for no steps to be taken”. The ALRC bolstered its recommendation with the observation that it is consistent with Principle 2 and the privacy legislation of New Zealand.¹⁷

3.28 In addition to its recommendation for legislative clarification, the ALRC recommended that the Office of the Federal Privacy Commissioner (“OPC”) develop and publish guidance on specific circumstances when it would be reasonable for no steps to be taken to notify individuals about the collection of their personal information. The ALRC recommended that the OPC guidance should specifically address areas identified by the submissions as needing clarification, as well as areas recognised in other jurisdictions as being appropriately excluded from the coverage of the obligation to take reasonable steps. These include when:

- notification would prejudice the purpose of collection, for example, when it would prejudice:
 - the prevention, detection, investigation and prosecution of offences;
 - legal action for breaches of a law imposing a penalty or seriously improper conduct;
 - the enforcement of laws; or
 - the protection of the public revenue;
- collection of personal information is required or authorised by or under law for statistical or research purposes;
- the personal information is collected from an individual on repeated occasions;
- an individual has been made aware of the relevant matters by the agency or organisation which disclosed the information to the collecting agency or organisation;
- non-compliance with the principle is authorised by the individual concerned;
- non-compliance with the principle is required or authorised by or under law;

17. ALRC Report 108 vol 1 [23.48]-[23.49].

- notification would pose a serious threat to the life or health of any individual; and
- health services collect family, social or medical histories.¹⁸

3.29 In NSW, s 10 of PPIPA and HPP 4 both refer to an obligation to take reasonable steps to ensure that the individual whose personal information has been collected has been made aware of specified matters. Like NPP 1.3, they do not include the phrase “if any” in relation to the taking of reasonable steps. Consequently, it is arguably uncertain whether agencies under PPIPA and organisations under HRIPA are authorised to decide that, in certain circumstances, it would be reasonable to take no steps to make an individual concerned aware of the matters listed in s 10 and HPP 4.

3.30 The Commission supports the recommendation of the ALRC that UPP 3 should provide that an agency or organisation is obliged to take “such steps, if any, as are reasonable in the circumstances” to notify or otherwise ensure that an individual is aware of specified matters. The recommended wording of UPP 3 clarifies that the obligation embodied in the notification principle is not absolute since there will be situations where entities that collect personal information would be justified in not notifying or ensuring the awareness by an individual of the matters listed in the principle. This recommendation, in tandem with the ALRC recommendation that the OPC issue guidance on specific circumstances when it would be reasonable for no steps to be taken to notify individuals about the collection of their personal information, effectively provides the basis for exemptions from compliance with the notification principle.

EXEMPTIONS

3.31 The ALRC examined whether the notification principle should spell out the circumstances in which an agency or organisation will not be required to comply with the principle.

3.32 In relation to this issue, the ALRC, in its DP 72, made several proposals, namely that:

- agencies that collect personal information — whether directly from an individual or from someone other than the individual — should not be required to comply with the notification requirements if they

18. ALRC Report 108 vol 1 [23.50], Recommendation 23.3(a).

are required or specifically authorised by or under law not to make the individual aware of one or more of the matters to be notified;¹⁹

- agencies and organisations that collect personal information — whether directly from an individual or from someone other than the individual — should be required to comply with the notification requirements only in circumstances where a reasonable person would expect to be notified; and²⁰
- agencies and organisations that collect personal information — whether directly from an individual or from someone other than the individual — should be required to comply with the notification requirements except to the extent that making the individual aware of the specified matters would pose a serious threat to the life or health of any individual.²¹

3.33 In addition, the ALRC considered whether the notification principle should contain an exception relating to when personal information is collected for statistical purposes or research. This was a suggestion made by the Australian Bureau of Statistics (“ABS”), which said that it often collects information in relation to individuals other than from the individuals themselves, for example in the Census, where one person in a household may complete the form for the entire household. The ABS argued that a requirement to notify the individuals concerned when information about them is collected from another person would put a very heavy administrative burden on the ABS.²²

3.34 In Report 108, the ALRC decided against incorporating in the notification principle specific circumstances in which an agency or organisation will not be required to comply. It reasoned that to do so would effectively incorporate detailed and prescriptive rules on the application of the principle, which would be inconsistent with the high-level principles approach it has adopted. Further, it argued that the provision for a limited number of exceptions to the principle might create a legitimate expectation that other circumstances will also be made the subject of an exception. The ALRC said that this “is likely to result in a

19. Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No 72 (2007) (“ALRC DP 72”) Proposals 20-4, 20-5(b)(iii).

20. ALRC DP 72 Proposals 20-2(1), 20-5(b)(i).

21. ALRC DP 72 Proposals 20-2(2), 20-5(b)(ii).

22. ALRC Report 108 vol 1 [23.67]-[23.68].

proliferation of legislative exceptions, fundamentally at odds with a principles-based approach”.²³

3.35 Instead of recommending legislative exceptions to the notification principle, the ALRC highlighted its recommendation that the OPC develop and publish guidance on the types of circumstances in which it may be reasonable for an agency or organisation to take no steps to notify individuals about the collection of their personal information.²⁴

The law in NSW

3.36 In NSW, s 10 of PPIPA itself does not contain exemptions. However, various other sections of PPIPA (which are located in its Division titled “Specific exemptions from principles”) provide exemptions from compliance with s 10, including where:

- the personal information concerned is collected for law enforcement purposes (whether or not the agency collecting the information is a law enforcement agency);²⁵
- compliance by an investigative agency with s 10 might detrimentally affect (or prevent the proper exercise of) the agency’s complaint handling functions or any of its investigative functions;²⁶
- the agency that collects the information is the Ombudsman’s Office;²⁷
- the agency is lawfully authorised or required not to comply with the principle concerned;²⁸ and
- non-compliance with s 10 is permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).²⁹

23. ALRC Report 108 vol 1 [23.70].

24. ALRC Report 108 vol 1 [23.71]-[23.74], Recommendation 23-3. See also para 3.24-3.30.

25. *Privacy and Personal Information Protection Act 1998* (NSW) s 23(3). However, this subsection does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.

26. *Privacy and Personal Information Protection Act 1998* (NSW) s 24(1).

27. *Privacy and Personal Information Protection Act 1998* (NSW) s 24(6).

28. *Privacy and Personal Information Protection Act 1998* (NSW) s 25(a).

29. *Privacy and Personal Information Protection Act 1998* (NSW) s 25(b).

3.37 In contrast to s 10 of PPIPA, HPP 4 contains exemptions in the principle itself. Its sub-clause (4) provides:

- (4) An organisation is not required to comply with a requirement of this clause if:
 - (a) the individual to whom the information relates has expressly consented to the organisation not complying with it, or
 - (b) the organisation is lawfully authorised or required not to comply with it, or
 - (c) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or
 - (d) compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates, or
 - (e) the information concerned is collected for law enforcement purposes, or
 - (f) the organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of its investigative functions.

The Commission's conclusion

3.38 The issue at hand is whether the notification principle should spell out exemptions from compliance with its provisions or whether such exemptions should be located elsewhere.

3.39 The ALRC has adopted a high-level principles approach in crafting the UPPs, which has the advantage of greater flexibility and adaptability. High-level privacy principles can more readily accommodate unforeseen circumstances and new technologies.³⁰ Such approach means minimising the inclusion of detailed and prescriptive rules in the privacy principles. In line with this approach, the ALRC has taken the view that UPP 3 should not spell out the specific circumstances in which an agency or organisation will not be required to comply. Instead, the exemptions would be addressed through its recommendation that the OPC issue guidance on specific circumstances when it would be reasonable for no

30. See ALRC Report 108 vol 1 Ch 18.

steps to be taken to notify individuals about the collection of their personal information.

3.40 In the Introduction to this Report, the Commission recorded its general agreement with the ALRC's view that principles-based regulation, which is complemented by specific rules in delegated legislation, should be the primary method for regulating information privacy in Australia.³¹ Consistent with this approach, the Commission supports the ALRC's decision not to include specific exemptions in UPP 3. Should this principle be adopted in NSW, the current exemptions found in s 10 of PPIPA and HPP 4 will need to be relocated in delegated legislation such as regulations or, as recommended by the ALRC, in guidelines issued by the Privacy Commissioner.

3.41 The ALRC identified some of the circumstances that would potentially be exempted from the notification principle under the OPC guidelines and some of them reflect the exemptions found in s 10 of PPIPA and HPP 4, including where:

- the collection of personal information is for law enforcement and investigative purposes;
- the collection of personal information is required or authorised by or under law;
- non-compliance with the principle is required or authorised by or under law;
- non-compliance with the principle is authorised by the individual concerned; or
- compliance with the notification principle would pose a serious threat to the life or health of any individual.

3.42 There are other circumstances which the ALRC has recommended for inclusion in the OPC guidelines, and which are not currently the subject of exemption under s 10 of PPIPA or HPP 4, such as where:

- the personal information is collected from an individual on repeated occasions; or
- an individual has been made aware of the relevant matters by the agency which disclosed the information to the collecting agency.

31. Para 0.5-0.9.

3.43 We agree that these matters ought to be considered for exemption from the notification principle under NSW law.

COLLECTION OF PERSONAL INFORMATION FROM A THIRD PARTY

3.44 There is currently a lack of consistency under the Privacy Act as to whether the notification obligations apply where the personal information is collected from someone other than the person to whom the information relates.

3.45 Principle 2 requires agencies to ensure that individuals are aware of specified matters relating to the collection of their personal information only where they collect the information from the individual concerned.

3.46 In contrast, NPP 1.3 requires organisations to ensure that individuals are aware of specified matters relating to the collection of their personal information, regardless of whether the information is collected directly from the individual or from someone other than the individual. Where an organisation collects information about an individual from someone else, the organisation may be exempted from the notification obligations to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.³²

3.47 In Report 108, the ALRC recommended that agencies and organisations should be subject to an obligation to notify an individual of, or otherwise ensure an individual's awareness of, specified matters relating to the collection of his or her personal information, regardless of whether that information is collected directly from the individual or from someone other than the individual.³³

3.48 The ALRC noted that this obligation already applies to organisations. It emphasised the point that under UPP 3, agencies and organisations may under certain circumstances have to assess whether it will be reasonable, in exercising any of their functions, not to take any steps to notify individuals about the collection of their personal information.³⁴

32. *Privacy Act 1988* (Cth) sch 3, NPP 1.3, 1.5.

33. ALRC Report 108 vol 1 [23.90], Recommendation 23-2.

34. ALRC Report 108 vol 1 [23.91].

3.49 Moreover, it recommended that the OPC develop and publish guidance on the specific circumstances where it would not be reasonable to provide notification where personal information has been collected from a third party, including where:

- the collection of personal information is required or authorised by or under law for statistical or research purposes;
- notification would pose a serious risk to the life or health of any individual; or
- health services collect family, social or medical histories.³⁵

The law in NSW

3.50 In NSW, s 10 of PPIPA provides that “[i]f a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that ... the individual to whom the information relates is made aware of” certain matters. By its terms, s 10 does not apply where the agency collects personal information from a person other than the person to whom the information relates.

3.51 This has been confirmed in *HW v Director of Public Prosecutions (No 2)*,³⁶ where the Administrative Decisions Tribunal held that s 10 only applies where an agency “collects personal information from an individual” to whom the information relates, not in relation to personal information from any individual. The Tribunal stated that:

One of the purposes of section 10 is to enable an individual to be fully informed of the relevant factors before deciding whether to provide the information to the agency. This would not be a relevant consideration if the information is collected from a third party, and the individual to whom the information relates is separately informed of the collection.³⁷

3.52 HPP 4 takes a different approach to s 10. HPP 4(1) requires an organisation that “collects health information about an individual from the individual” to take reasonable steps to ensure that the individual is aware of certain matters. However, HPP 4(2) provides that where “an organisation collects health information about an individual from

35. ALRC Report 108 vol 1 [23.92], Recommendation 23.3(a).

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

37. *HW v The Director of Public Prosecutions (No 2)* [2004] NSWADT 73 [23].

someone else”, it must take reasonable steps to ensure that the individual is generally aware of the matters listed in subclause (1), except to the extent that this would pose a serious threat to the life or health of any individual; or the collection is exempted from compliance by guidelines issued by the Privacy Commissioner.

Submissions

3.53 In CP 3, we proposed that s 10 of PPIPA be amended to stipulate that its requirements apply whether the information is collected directly from the individual to whom the information relates or indirectly from someone else. We also queried whether s 10 should be amended to adopt the wording of HPP 4 or UPP 3, or some combination of the two.³⁸

3.54 A number of submissions supported the idea that the notification requirements should apply whether the personal information is collected directly from the individual to whom the information relates or indirectly from someone else.³⁹ The Australian Privacy Foundation and the Cyberspace Law and Policy Centre preferred the approach proposed in UPP 3.⁴⁰

3.55 The Inner City Legal Centre also supported the proposal and said that the protections contained in s 10 of PPIPA would be significantly undermined if they did not apply to personal information that is indirectly collected. Further, it said that an individual would be “at a significant disadvantage in terms of correcting inaccuracies or complaining about misuse or disclosure of personal information if these fundamental principles do not apply to indirect collection”.⁴¹

3.56 The NSW Department of Corrective Services was the only agency that opposed the proposal, arguing that it is impractical.⁴²

38. NSW Law Reform Commission, *Privacy Legislation in New South Wales*, Consultation Paper No 3 (2008) Proposal 10, Issue 33.

39. Australian Privacy Foundation, *Submission*, 8; Cyberspace Law and Policy Centre, *Submission*, 21; Inner City Legal Centre, *Submission*, 15.

40. Australian Privacy Foundation, *Submission*, 8; Cyberspace Law and Policy Centre, *Submission*, 21.

41. Inner City Legal Centre, *Submission*, 15.

42. NSW Department of Corrective Services, *Submission*, 2.

The Commission's conclusion

3.57 The NSW privacy legislation should incorporate the provisions of UPP 3 relating to the obligation of entities that collect personal information to notify an individual of, or otherwise ensure an individual's awareness of, specified matters relating to the collection of his or her personal information, regardless of whether that information is collected directly from the individual or from someone other than the individual.

3.58 The Commission agrees with the statement of the Administrative Decisions Tribunal in *HW v Director of Public Prosecutions (No 2)* that one of the functions of the notification requirements is to enable an individual to be fully informed of the relevant factors before deciding whether to provide the information to the agency. However, the Commission considers that the notification requirements perform other functions, including informing those whose personal information has been collected the legal basis and purpose of the collection; their rights to access and, if appropriate, their rights to correct the information; and the availability of avenues of complaints. These matters are relevant not only to individuals who provide the information themselves but also to those whose personal information was given to an agency by a third party. It is arguable, for example, that the chances that the information may not be accurate, complete or up-to-date are higher where the information was provided by a third party than where the information was given directly by the person to whom the information relates. The individual whose personal information was collected from a third party should therefore be able to examine its quality and accuracy and request its correction, if appropriate.

3.59 There are, of course, situations where an agency collects information from a third party and it would not be appropriate to notify the individual concerned about the collection, for example, in criminal investigations. UPP 3 provides for such situations by allowing agencies to determine whether it will be reasonable in the circumstances not to take any steps to notify individuals about the collection of their personal information.

CONTENT OF NOTIFICATION

3.60 This section examines each of the items in UPP 3 that are the subject of the notification principle.

The fact and circumstances of collection

3.61 The Principles and NPPs under the Privacy Act do not require an agency or organisation to notify an individual that it has collected, or is about to collect, personal information about that individual.

3.62 The ALRC recommended that:

Agencies and organisations should be required to notify or otherwise ensure that an individual is aware of the fact and circumstances of the collection of his or her personal information *where the individual may not be aware of such collection*. Circumstances of collection may include how and when the information was collected.⁴³

3.63 The recommendation addresses the situation where an individual is not aware that his or her personal information has been collected. The ALRC is particularly concerned about new technologies that allow the collection of personal information without the knowledge of the individual concerned. These include invisible information collecting devices on web pages (such as “cookies”), hidden radio frequency identification (RFID) tags, and biometric systems such as facial and voice recognition devices.⁴⁴

3.64 The ALRC said that it is important for individuals to know the fact and circumstances of the collection of their personal information to enable them to exercise any rights relating to that information, for example, those relating to access and correction. It added that such a requirement promotes transparency in the collection practices of agencies and organisations.⁴⁵

3.65 The ALRC decided that where it is clear that an individual is aware that his or her personal information has been collected — for example, where an individual voluntarily provides the personal information — the collector of the information need not notify the individual about the fact and circumstances of the collection. The ALRC asserted that, if the individual is already aware of the collection, it would be superfluous to notify him or her of such collection. Further, it said that “the provision of such information could detract the individual’s attention from other important information relating to the collection, required to be provided

43. ALRC Report 108 vol 1 [23.108] emphasis added.

44. ALRC Report 108 vol 1 [23.104]-[23.105], [23.109].

45. ALRC Report 108 vol 1 [23.109].

by the agency or organisation, of which he or she is not aware”. Finally, the ALRC agreed with the argument in some of the submissions it received that imposing an obligation on agencies and organisations that is arguably unnecessary would not be cost effective since it would increase compliance costs but deliver very little additional privacy protection.⁴⁶

3.66 In NSW, s 10(a) of PPIPA provides that “the fact that the information is being collected” should be among the matters that agencies should ensure that the individual concerned is made aware. This provision is different from UPP 3(a) in two respects. First, it covers the fact, but not the circumstances, of the collection. Secondly, it is not confined to situations “where the individual may not be aware that his or her personal information has been collected”.

3.67 In contrast to s 10(a) and UPP 3(a), HPP 4 does not contain an equivalent provision.

3.68 The Commission supports the ALRC’s recommendation. A requirement similar to the one in s 10(a) that the individual concerned should be made aware of the fact that his or her personal information has been collected is largely superfluous since the privacy notice (or other means of achieving awareness of the collection) that is to be provided to such individual would necessarily imply this fact. When being notified about the identity and contact details of the collector; the purpose and legal basis of the collection; that he or she may request access to and (if appropriate) correction of the information; and that there are avenues for complaint relating to the collection and handling of personal information — the individual would inevitably become aware that his or her personal information is being, or has been, collected. The usefulness of the information about the fact of collection lies mainly in providing a premise for the other matters that are subject of the notification principle.

3.69 In comparison, the additional requirement in UPP 3(a) that the individual be informed about the circumstances of the collection is of greater significance. This is because it would allow the individual to assess whether the collector has complied with requirements relating to collection, in particular UPP 2.2, which requires the collector to “collect personal information only by lawful and fair means and not in an unreasonably intrusive way”. Hence, by covering both the fact and

46. ALRC Report 108 vol 1 [23.110].

circumstances of collection, UPP 3(a) is an improvement on the requirement found in s 10(a) of PPIPA.

3.70 The Commission agrees, in principle, with the qualification in UPP 3(a) that agencies and organisations should be required to notify an individual, or otherwise ensure that an individual is aware, of the fact and circumstances of the collection of his or her personal information only where the individual may not be aware of such collection. We agree with the ALRC's argument that, where the individual is already aware of the collection, it may be redundant to notify him or her of such collection. It must, however, be acknowledged that it will not always be certain whether the individual concerned is, in fact, aware that his or her personal information has been collected. In the Commission's view, the safe approach is for agencies and organisations to take steps, as a matter of course, to ensure that the individual is notified, or made aware of the fact and circumstances, of the collection of his or her information. It is doubtful whether the provision of such information would necessarily involve unreasonable costs to the agency or organisation.

Collector's identity, individual's rights, and consequences of not providing information

3.71 NPP 1.3 contains obligations relating to notification of: (a) the collector's identity, (b) an individual's rights relating to access, and (c) the main consequences of not providing the information. The Principles do not impose any of these obligations on agencies. The ALRC recommended that such obligations should also apply to agencies.

Collector's identity and contact details

3.72 The ALRC recommended that agencies and organisations should have an obligation to inform individuals of the identity and contact details of the agency or organisation that collected the personal information. It reasoned that individuals should know whom to contact in order to exercise any rights that they may have relating to their personal information, and the means by which contact can be made.⁴⁷

3.73 The recommended obligation is currently already reflected in s 10(f) of PPIPA and HPP 4(a). There are no policy reasons why this specific obligation should be abolished in NSW. The provision of information about the identity and contact details of the entity that

47. ALRC Report 108 vol 1 [23.120].

collects the personal information is fundamental to the ability of individuals to take measures to protect, or otherwise to make decisions about, their personal information.

Access and correction rights

3.74 The ALRC recommended that the notification principle include an obligation to inform individuals about their rights under the UPPs to access, and correct, their personal information. It said that awareness of such rights is essential to encouraging individuals to exercise those rights to ensure the accuracy of their personal information. Further, it said that this particular notification obligation complements the ‘Data Quality’ Principle, which obliges collectors of personal information to make sure that the information they collect is accurate, complete, up-to-date and relevant.⁴⁸

3.75 This recommendation is already reflected in s 10 of PPIPA.⁴⁹ In comparison, HPP 4 lists “the fact that the individual is able to request access to the information”⁵⁰ but does not mention the fact that the individual can also request correction of the information.

3.76 The Commission supports this recommendation for the reasons given by the ALRC. Should it be adopted in NSW, the recommendation would improve the notification principle as it relates to health information, since individuals whose health information is collected would need to be informed that they are able not just to access but also to correct such information, in case it is inaccurate, incomplete or out-of-date.

Consequences of not providing information

3.77 The ALRC said that individuals should be entitled to know the main consequences of not providing their personal information, for example, that it may result in the individual not being able to access a service or benefit.⁵¹ Accordingly, UPP 3(e) provides that the notification obligations should include information about the “main consequences of not providing the information”.

48. ALRC Report 108 vol 1 [23.121].

49. *Privacy and Personal Information Protection Act 1998* (NSW) s 10 (e).

50. *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPP 4(b).

51. ALRC Report 108 vol 1 [23.122].

3.78 Section 10 of PIPPA and HPP 4 both contain the substance of this recommendation but their wording is more precise than that found in UPP 3.

- Section 10(d) contains the words: “any consequences for the individual if the information (or any part of it) is not provided”.
- HPP 4(c) states: “the main consequences (if any) for the individual if all or part of the information is not provided”.

3.79 These provisions contain two points that are not clearly dealt with in UPP 3(e). First, the phrase “if any” in HPP 4(c) expressly covers the situation where there are no consequences arising from the information not being provided, in which case there is no need to comply with this particular requirement. Secondly, both provisions cover the situation where only part of the information is not provided and there are consequences arising from this. The Commission considers that UPP 3(e) should be reworded to cover these situations.

RECOMMENDATION 4

UPP 3(e) should be modified in the following way:

UPP 3. Notification

At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of, the:

...

(e) main consequences (*if any*) of not providing *all or part of* the information.

Purposes for which information is collected

3.80 Principle 2(c) and NPP 1.3(c) require agencies and organisations to ensure that an individual is aware of the purposes for which his or her personal information is collected.

3.81 The ALRC recommended that this obligation should continue to be included in the UPPs, simply stating that there is no policy reason to amend or remove it.⁵²

52. ALRC Report 108 vol 1 [23.129].

3.82 Some of the submissions it received expressed concern about compliance with this obligation in circumstances where there are several purposes. The ALRC said that, if the collector of the information knows at the time of collection that it intends to use the information for other purposes related to the main purpose of collection, it should make the individual aware of these related purposes. The ALRC noted that this issue is already the subject of guidance from the OPC.⁵³

3.83 In NSW, both s 10 of PPIPA and HPP 4 require agencies and organisations to ensure that an individual is aware of the purposes for which his or her personal information is collected.⁵⁴

3.84 The Commission supports the ALRC's recommendation to maintain the obligation to inform individuals of the purposes for which their personal information is collected. Under the purpose specification principle, which is one of the core principles of data protection under the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,⁵⁵ collection of personal data or information must be for specified purposes and the subsequent use is limited to the fulfilment of those purposes or such others as are not incompatible with those purposes. The recommendation under consideration is one of the means of implementing this core principle.⁵⁶ The information about the purposes of the collection enables the individuals concerned to take measures to protect their personal information, including withholding it if they do not agree with the specified purposes, or making a complaint if the information is used for purposes other than the specified purposes.

53. ALRC Report 108 vol 1 [23.130].

54. *Privacy and Personal Information Protection Act 1998* (NSW) s 10(a); *Health Records and Information Privacy Act 2002* (NSW) sch 1 HPP 4(1)(c).

55. Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) Guideline 9. The preamble to the *Privacy Act 1988* (Cth) states that Australia is a member of the OECD; that the Council of the OECD has recommended that member countries take into account in their domestic legislation the privacy principles set out in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); and that Australia has expressed its intention to participate in the recommendation. See also United Nations, *Guidelines Concerning Computerized Personal Data Files* (1990) Principle 3.

56. See also Chapters 2 (Collection) and 5 (Use and Disclosure) of this Report.

Entities to which information is usually disclosed

3.85 Principle 2(e) requires agencies to ensure that an individual whose personal information has been collected is generally aware of:

any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

3.86 NPP 1.3(d), on the other hand, requires organisations to ensure that an individual whose personal information has been collected is aware of:

the organisations (or the types of organisations) to which the organisation usually discloses information of that kind.

3.87 The ALRC's recommendation on this matter is encapsulated in UPP 3(h), which requires agencies and organisations to ensure that an individual whose personal information has been collected is aware of:

actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information of the kind collected.

3.88 UPP 3(h) extends the notification obligations of organisations by covering not just other organisations but also agencies, entities and other persons to whom the collector-organisation usually discloses personal information of the kind collected. The ALRC asserted that it is important to present individuals whose personal information has been collected with a complete picture of the collector's usual disclosures to enable them to make informed decisions about protecting their personal information.⁵⁷

3.89 UPP 3(h) also clarifies that agencies and organisations are required to inform individuals of the actual, as well as *types* of, entities to which they disclose personal information. The ALRC observed that this is consistent with current guidance from the OPC, which allows general descriptions of sets of people and organisations (for example, "State Government licensing authorities" and "State police forces").⁵⁸

57. ALRC Report 108 vol 1 [23.144].

58. ALRC Report 108 vol 1 [23.143].

3.90 The ALRC commented that the specificity of the information needed to comply with this requirement would depend on the particular circumstances. It said that there is “a need to strike a balance between providing useful and digestible information to an individual and ensuring that the costs and compliance burden in meeting the obligation are not unduly onerous”. It recommended that the OPC develop and publish guidance on the appropriate level of specificity when notifying individuals about the entities to which personal information of the kind is usually disclosed.⁵⁹

3.91 In NSW, HPP 4(d) refers to “the persons to whom (or the types of persons to whom) the organisation usually discloses information of that kind”. This provision is very similar to UPP 3(h). In relation to personal information other than health information, s 10(c) of PPIPA, which refers to “the intended recipients of the information”, appears to be the comparable provision.

3.92 The Commission supports the ALRC recommendation. It would be onerous and, in many cases, impractical to require entities that collect personal information to inform individuals to whom the information will actually be disclosed since this may not be known at the time of notification. It is more pragmatic to require the collecting entity to ensure the awareness of individuals concerned about the actual and types of entities to whom the agency or organisation usually discloses personal information of the kind collected. Such information, together with the other matters that are subject of the notification principle, should be sufficient to assist individuals in taking measures to safeguard their personal information if they deem it necessary or desirable in the circumstances. It should also be noted that, as indicated above, the ALRC’s recommendation is already reflected in the NSW requirements relating to health information.

Avenues of complaint

3.93 The Principles and NPPs do not currently require an agency or organisation to notify an individual whose personal information is being, or has been, collected of the avenues of complaint if he or she has a privacy complaint.

59. ALRC Report 108 vol 1 [23.145]-[23.146].

3.94 The ALRC, in its examination of the openness principle, recommended that each agency and organisation should produce a written and publicly available Privacy Policy that sets out its policies on how it manages the personal information it collects. The avenues of complaint available to individuals in the event that they have a privacy complaint are among the matters that the ALRC recommended for inclusion in the Privacy Policy.⁶⁰

3.95 In addition, the ALRC considered it important that, at or about the time personal information is collected, the individual concerned be notified, or otherwise made aware, of the fact that there are avenues of complaint available in the event that they have a privacy complaint. It said that this would promote accountability and transparency, and help create a regulatory environment where individuals are aware that they may take steps to protect their personal information.⁶¹

3.96 The ALRC, however, considered it unnecessary for an individual to be notified or made aware of the actual avenues of complaint at the time of the collection of his or her personal information. It said that this notice should be located more appropriately in the Privacy Policy of the agency or organisation.⁶² The ALRC was concerned about putting any unnecessary detail in privacy notices.⁶³ Consequently, it recommended that the fact that there are avenues of complaint available to individuals, and that these are set out in the agency's or organisation's Privacy Policy, should be among the subject matters for notification.⁶⁴

3.97 There is currently no provision in the relevant NSW statutes that is the equivalent of the ALRC recommendation.

3.98 The Commission is strongly in favour of informing individuals whose personal information is collected that there are avenues for complaint with respect to the collection or handling of the information. It also agrees with the ALRC's view that it is important to minimise the danger of overloading individuals with too much information in the privacy notices since this can impinge on their capacity and willingness to process and retain such information. It is sufficient for the collector of

60. ALRC Report 108 vol 1 Recommendation 24-1.

61. ALRC Report 108 vol 1 [23.153].

62. ALRC Report 108 vol 1 [23.154].

63. ALRC Report 108 vol 1 [23.152].

64. ALRC Report 108 vol 1 [23.154].

information to inform individuals at the notification stage about the availability of avenues of complaint and to refer them to its Privacy Policy, which will have details of the avenues of complaint.⁶⁵

Information required or authorised by or under law

3.99 Both the Principles and NPPs contain a notification requirement about the legal basis of the collection of personal information. However, the relevant Principle and NPP are worded differently.

3.100 Pursuant to Principle 2(d), agencies are required, where applicable, to ensure that individuals whose personal information has been collected are aware of “the fact that collection of information is authorised or required by or under law”.

3.101 NPP 1.3(e), on the other hand, requires organisations to ensure that individuals whose personal information has been collected are aware of “any law that requires the particular information to be collected”.

3.102 The OPC’s guidance on Principle 2(d) states:

An IPP 2 notice should refer to each provision of legislation which:

- requires an agency to collect the personal information; or
- specifically authorises an agency to collect the information.

If legislation does not refer to a specific power, but only gives the agency a general function which includes collecting personal information, the IPP 2 notice should still refer to the legislation.⁶⁶

3.103 The OPC’s guidance on NPP 1.3(e) provides that:

In describing the law the organisation need not specify the exact piece of legislation (although it would be desirable to do so where possible). A statement like ‘taxation law requires us to collect this’ would ordinarily be adequate.⁶⁷

65. See para 4.15-4.20.

66. Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994) 17.

67. Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001) 31.

3.104 The ALRC considered it important to retain an obligation relating to notification of the legal basis for the collection of personal information and said that the obligation should be standardised for agencies and organisations.⁶⁸

3.105 It said that the wording of Principle 2(d) is of particular relevance to the many agencies that have coercive information-gathering powers. Consequently, it concluded that, from a practical point of view, it is appropriate to use Principle 2(d) as the template for drafting this particular obligation. UPP 3(h) therefore requires agencies and organisations to notify an individual, or otherwise ensure that an individual is aware, of the “fact, where applicable, that the collection is required or authorised by or under law”.

3.106 The ALRC also recommended that the OPC develop and publish guidance as to what would be required of organisations as a result of the recommended redrafting of the obligation as it applies to them.⁶⁹

3.107 In NSW, the relevant provisions refer to the law that requires the collection.

- Section 10(d) of PPIPA uses these words: “whether the supply of the information by the individual is required by law”.
- HPP 4(d) states: “any law that requires the particular information to be collected”.

3.108 The Commission supports the wording in UPP 3, which is more comprehensive than the NSW provisions since it covers situations where a law authorises, but does not necessarily require, the collection of the information. As the ALRC pointed out, such situations are of particular relevance to agencies that are authorised by or under law to collect personal information as part of their regulatory or law enforcement functions.

68. ALRC Report 108 vol 1 [23.158].

69. ALRC Report 108 vol 1 [23.161].

4. UPP 4: Openness

- ALRC Report 108
- NSWLRC's Consultation Paper 3
- Conclusion

4.1 The principle of “openness” is concerned with the transparency of the information-handling practices of agencies. That is, it focuses on the ability of the public, specifically those whose personal information has been collected by an agency, to know what the agency’s practices are in relation to information collection and handling. How open is the agency in revealing to the public how it collects personal information and what does it do with it?

ALRC REPORT 108

Model Unified Privacy Principle 4

4.2 In its Report 108, the ALRC noted that both the Principles and the NPPs set out in the Privacy Act¹ already contain openness requirements,² though not an overarching principle. The openness requirements are contained in Principle 5 and NPP 5.

4.3 Principle 5 addresses both openness and notification requirements. Principle 5.1 provides that a record-keeper in possession or control of records containing personal information must take reasonable steps to enable any person to find out whether such records are held in relation to him or herself and, if so:

- the nature of the information;
- the main purposes for which it is used; and
- how to go about obtaining access to the records.³

4.4 This obligation is not limited to where the person has made a request, unlike the comparable obligation in NPP 5. The record-keeper must keep a register of all records of personal information detailing:

- the nature of the records;
- the purpose for which each is kept;
- the classes of individuals about whom records are kept;

-
1. The Principles are set out in s 14 of the *Privacy Act 1988* (Cth) and the NPPs are set out in Schedule 3 to the Act.
 2. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) vol 1 [24.2].
 3. Unless the record-keeper is required or authorised under a Commonwealth law regulating access to documents to refuse to give out the information: UPP 5.2.

- how long each record is kept; who can have access and under what conditions; and
- how access can be gained.⁴

This register must be available for inspection by the public and a copy must be given to the Office of the Federal Privacy Commissioner (“OPC”) annually.⁵

4.5 NPP 5 provides that an organisation must have a document that clearly sets out its personal information management policies, and that this must be made available to anyone who asks for it.⁶ This is a more generally expressed obligation than the one in Principle 5, which, as noted above, prescribes specific matters that must be included in the register of records. NPP 5 further provides that anyone who asks what sort of personal information the organisation holds, and for what purposes, and how the organisation collects, holds, uses and discloses that information, must be told.⁷

4.6 The ALRC concluded that principles addressing openness and notification requirements⁸ should not be bundled into one.⁹ It recommended that the UPPs contain a discrete openness principle, unequivocally identified by being styled “Openness”,¹⁰ addressing the need for an agency or organisation to operate openly and transparently.¹¹

4.7 The recommended openness principle, UPP 4, requires that an agency or organisation put in place:

a Privacy Policy that sets out clearly its expressed policies on the management of personal information, including how it collects, holds, uses and discloses personal information. This document should also outline the:

- (a) sort of personal information the agency or organisation holds;

4. Principle 5.3.

5. Principle 5.4.

6. NPP 5.1

7. NPP 5.2

8. See ALRC Report 108 vol 1 UPP 3.

9. ALRC Report 108 vol 1 [24.9]-[24.12].

10. ALRC Report 108 vol 1 [24.913].

11. ALRC Report 108 vol 1 Recommendation 24-1, UPP 4. The notification principle is UPP 3, discussed in Chapter 3.

- (b) purposes for which personal information is held;
- (c) avenues of complaint available to individuals in the event that they have a privacy complaint;
- (d) steps individuals may take to gain access to personal information about them held by the agency or organisation; and
- (e) whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.¹²

4.8 UPP 4 further provides that:

An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual:

- (a) electronically; and
- (b) on request, in hard copy, or in an alternative form accessible to individuals with special needs.¹³

4.9 The ALRC also recommended that the OPC “encourage and assist agencies and organisations to make available short form privacy notices summarising their personal information-handling practices”,¹⁴ and that these be “seen as supplementing the more detailed information that is required to be made available to individuals under the Privacy Act”.¹⁵

The rationale behind Recommendation 24-1

A discrete principle

4.10 First, the ALRC was of the view that it was “not appropriate to deal with requirements relating to openness and notification in the same principle because of their important conceptual differences”.¹⁶ On the one hand, openness provisions benefit the public at large by enabling anyone at all to discover what an organisation’s general practices and policies are for the handling of personal information. On the other hand, “notification requirements” refer to an organisation’s obligation to notify a particular

12. ALRC Report 108 vol 1 UPP 4.1, Recommendation 24-1.

13. ALRC Report 108 vol 1 UPP 4.2, Recommendation 24-1.

14. ALRC Report 108 vol 1 Recommendation 24-3.

15. ALRC Report 108 vol 1 Recommendation 24-3.

16. ALRC Report 108 vol 1 [24.10].

individual that the organisation plans to collect, or has collected, personal information about him or her, and make that individual aware of certain matters relating to the use and handling of his or her personal information. The requirement is for the exclusive benefit of the individual whose personal information is being collected.¹⁷

4.11 The ALRC also took into account submissions to its DP 72.¹⁸ For example, the ALRC took note of the Public Interest Advocacy Centre’s view that a discrete principle would “serve to highlight the importance of this principle as a mechanism for ensuring open and transparent handling of personal information by agencies and organisations”.¹⁹ In addition, Privacy NSW put forward a compelling argument that an openness principle would not only “increase the transparency of organisations’ and agencies’ dealings with regard to ... personal information”, but would also “assist in identifying and remedying compliance issues”.²⁰

4.12 The ALRC concluded that a separate openness principle would promote “best practice in the handling of personal information”²¹ by enabling the OPC, and any other regulatory office or body, to examine privacy policies published in compliance with the openness UPP. An agency’s or organisation’s compliance with the Privacy Act could be monitored, and changes to practices and policies recommended as needed.²²

Formulation of the principle

4.13 The ALRC noted that Principle 5 and NPP 5 set out different regulatory mechanisms, the former being quite specific and the latter being more general.²³ As observed in paragraph 4.3, the obligations on an agency under Principle 5 are to enable anyone to find out certain

17. ALRC Report 108 vol 1 [24.10]-[24.11].

18. Australian Law Reform Commission, *Review of Australian Privacy Law* Discussion Paper 72 (2007) (“ALRC DP 72”).

19. Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007, cited in ALRC Report 108 vol 1 [24.8].

20. Privacy NSW, *Submission PR 468*, 14 December 2007 cited in ALRC Report 108, vol 1 [24.7].

21. ALRC Report 108 vol 1 [24.12].

22. ALRC Report 108 vol 1 [24.12].

23. ALRC Report 108 vol 1 [24.14]. See para 4.3-4.5 where these mechanisms are set out.

specified matters about the records of personal information it keeps, and to maintain a record, available for public inspection, setting out a number of specified matters relating to the agency's handling of personal information. This record must be given annually to the OPC, which uses it to create the Personal Information Digest.²⁴

4.14 In comparison, the obligations on an organisation under NPP 5 are to set out in a document, made available for public inspection, the organisation's policies on its management of personal information. A person who asks must be told, generally, what sort of personal information the organisation holds and for what purposes, and how it collects, holds, uses and discloses that information.

4.15 The ALRC examined the two contrasting mechanisms for achieving openness to determine the best model. It concluded that a general approach to regulating openness was to be preferred and proposed that:

the 'Openness' principle should set out the requirements on an agency or organisation to operate openly and transparently by providing general notification in a Privacy Policy of how it manages, collects, holds, uses and discloses personal information.²⁵

The proposal was widely supported²⁶ and incorporated in Recommendation 24-1.

4.16 Recommendation 24-1 abandons the Personal Information Digest required to be kept pursuant to IPP 5. This was in response to criticism that the mechanism was not operating successfully, was of limited utility and that the information could be disseminated better in other ways.²⁷ The ALRC concluded that the purpose of the Personal Information Digest could be achieved more effectively by each agency and organisation producing a written, publicly available, Privacy Policy. Eliminating the need to provide the OPC with records for the Personal Information Digest would also ease the compliance burden on agencies.²⁸

24. This is the record of personal information required to be maintained by a federal government agency pursuant to s 14 of the *Privacy Act 1988* (Cth), Principle 5, and provided to the Privacy Commissioner annually.

25. ALRC DP 72 Proposal 21-1.

26. See ALRC Report 108 vol 1 [24.18].

27. ALRC Report 108 vol 1 [24.16].

28. ALRC Report 108 vol 1 [24.21], [24.25].

4.17 The advantages of a Privacy Policy, in which an agency or organisation documents how personal information is to be collected, held, used and disclosed, include the following:

- The agency or organisation will by necessity focus on how the UPPs apply to its activities, and will structure its operation so as to comply with the UPPs.²⁹
- Accountability is promoted because the actual practices of the agency or organisation can be compared against the affirmed practices set out in the Privacy Policy.
- Transparency of the information-handling practices of particular agencies and organisations is increased.
- Individuals can make more informed choices about whether they wish to transact with particular agencies or organisations.

4.18 The matters that Recommendation 24-1 suggest should be contained in a Privacy Policy are less prescriptive than Principle 5 but more specific than NPP 5. It was felt that NPP 5 was too vague about what it required of organisations. Furthermore, the different purposes of an openness principle and a notification principle need to be considered and an appropriate balance struck between them. As the ALRC observed “[a]n assessment of the content of one principle cannot be made without reference to the other”.³⁰ As a notification principle is, as it arguably should be, relatively prescriptive, an openness principle should therefore be less so.³¹

4.19 The recommended UPP brings clarity to the openness obligations, but achieves a level of specificity that is in keeping with its purpose. Privacy Policies that end up being long and complex as a result of trying to comply with a prescriptive openness principle run the risk of overwhelming the customer and going unread.

4.20 The ALRC also concluded that it was appropriate to include in a Privacy Policy general information about the steps individuals may take to access and correct personal information, even though this is a matter dealt with in the notification principle. The former notifies members of the public of their rights; the latter instructs the individual “the process

29. ALRC Report 108 vol 1 [24.22].

30. ALRC Report 108 vol 1 [24.48].

31. ALRC Report 108 vol 1 [24.48]-[24.49].

by which that right can be exercised”.³² One “complements, but does not duplicate,” the other.³³ Likewise, notifying the public in the Privacy Policy what avenues of complaint are available to individuals “complements, but does not duplicate,” the inclusion of this matter in the notification principle.³⁴ However, in keeping with the high-level focus of the openness principle, the details of information to be provided about complaints-handling mechanisms should be a matter for guidelines, not the principle itself.³⁵

Discussion Paper 72

4.21 In DP 72, the ALRC had proposed that, in addition to the matters set out in (a)-(d) of Recommendation 24-1, three further matters should be addressed in a Privacy Policy. These were:

- the types of individuals about whom records are kept;
- the period for which each type of record is kept; and
- the person, other than the individual, who can access personal information and the conditions under which they can access it.³⁶

The inclusion of these additional matters was not supported in submissions to DP 72 and the ALRC abandoned them in the final recommendation.

4.22 Information about the types of individuals about whom records are kept, and access to personal information by persons other than the individual, were thought to be unnecessary, as this information can be gleaned from the agency’s or organisation’s purposes for handling personal information.³⁷ It can also be ascertained from a general description of the agency’s or organisation’s disclosure practices set out in its Privacy Policy, and from information provided in compliance with the notification principle.³⁸

32. ALRC Report 108 vol 1 [24.51].

33. ALRC Report 108 vol 1 [24.51].

34. ALRC Report 108 vol 1 [24.52].

35. ALRC Report 108 vol 1 [24.54].

36. ALRC DP 72 Proposal 21-2.

37. ALRC Report 108 vol 1 [24.57].

38. ALRC Report 108 vol 1 [24.57].

4.23 It was also decided that having to provide details in a Privacy Policy about retention periods for each type of record containing personal information might be too costly and burdensome.³⁹

4.24 The ALRC's final recommendation included a matter not originally proposed in DP 72. This was "whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred".⁴⁰ This was included in response to concerns expressed to the ALRC about agencies and organisations sending personal information overseas.⁴¹

NSWLRC'S CONSULTATION PAPER 3

4.25 There is no direct equivalent of UPP 4 in the IPPs contained in PPIPA nor in the HPPs contained in HRIPA, requiring the creation of a Privacy Policy. The closest equivalent principles are s 13 of PPIPA (IPP 6) and HPP 6.

4.26 IPP 6, "Information about personal information held by agencies", provides:

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

- (a) whether the agency holds personal information, and
- (b) whether the agency holds personal information relating to that person, and
- (c) if the agency holds personal information relating to that person:
 - (i) the nature of that information, and
 - (ii) the main purposes for which the information is used, and
 - (iii) that person's entitlement to gain access to the information.

39. ALRC Report 108 vol 1 [24.58].

40. ALRC Report 108 vol 1 Recommendation 24-1 (e).

41. The ALRC conducted a National Privacy Phone-in, which logged a large number of calls expressing concern about this matter: ALRC Report 108 vol 2 [31.232].

4.27 HPP 6 applies to health information in identical terms but allows an exception to compliance with the provision if non-compliance is lawfully authorised or required, or otherwise permitted under an Act or any other law.⁴² This exception is not present in IPP 6.

4.28 There is a fundamental difference between the proposed UPP 4 on the one hand and IPP 6 and HPP 6 on the other hand that gives these principles different roles and emphases. Pursuant to UPP 4, an agency or organisation informs the public at large of its information management policies and practices. Anyone at all can access the Privacy Policy to learn about how the agency or organisation collects, holds, uses and discloses personal information, the sort of personal information held and for what purpose, how to make a complaint, how to access information, and policies on overseas transfer of information.

4.29 In contrast, IPP 6 and HPP 6 make limited information available, to an individual who requests it, about whether it holds personal information generally and whether it holds personal information specifically in relation to that individual. It is only if there is information relating to that individual that he or she then has a right to ask what is the nature of that information, the main purposes for which it is used, and his or her entitlement to gain access. There is nothing in IPP 6 or HPP 6 that compels public disclosure of an agency's or organisation's information privacy policies and practices.

4.30 No issue was raised in relation to either IPP 6 or HPP 6 in CP 3 as both principles were seen by the Commission as effectively fulfilling their functions. No submissions raised the desirability of introducing a privacy principle, operating separately from IPP 6 and HPP 6, fulfilling a different, more general, role.

CONCLUSION

4.31 It is clear, then, that IPP 6 and HPP 6 do not perform the same function as UPP 4 and that there is no other equivalent principle in the State legislation.

4.32 PPIPA allows for the making of privacy codes of practice by public sector agencies⁴³ but they are rarely framed in terms akin to a Privacy

42. *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 6(2).

43. *Privacy and Personal Information Protection Act 1998* (NSW) Part 3 of Division 1.

Policy. The closest example is the Privacy Code of Practice for the NSW Public Sector Workplace Profile 2004. It sets out the management arrangements for the Profile, such as who has responsibility for managing and administering the Profile, and who can access information. It states what provisions, or types of information, are exempt from PPIPA; sets out the information that is to be covered by the Code; states the purpose of collection and to what use the information will be put; describes how the IPPs will apply and where they will vary; provides for what access an employee can have to his or her information, and what authorised officers, other agencies or authorities can have access; and addresses storage, transmission and alteration of information. In the main, however, privacy codes are formulated by an agency for the sole purpose of modifying or waiving the application of the IPPs to that agency. They contain no statement of the principle of openness, statement of policies, or statement of intention to operate openly and transparently.

4.33 The Commission supports the concept and formulation of UPP 4, and its adoption into NSW privacy legislation, for the following reasons.

4.34 The threshold reason to have an openness principle at all is to promote a culture of trust and reliability between the public, whose personal information is collected, used, stored and shared, and the agency who must handle that information in order to perform its function. The Commission fully supports transparency and openness in an agency's information-handling practices and policies, and supports the public's right to ascertain readily information regarding those practices and policies.

4.35 The Commission agrees with the ALRC that it is not appropriate merely to incorporate a principle of openness into the notification principle. The focus and role of each is quite different and should be distinguished from each other by being expressed in separate principles. As the ALRC noted, and as is explained more fully above, openness provisions benefit the public at large, whereas "notification requirements" are for the exclusive benefit of the individual whose personal information is being collected.

4.36 Furthermore, the Commission agrees with the identified advantages of a Privacy Policy and is of the view that this approach would work equally well for State agencies. We also agree with the balance struck between the prescriptiveness of Principle 5 and the generality of NPP 5.

4.37 As explained in the Introduction, the Commission supports national uniformity, where possible, in privacy laws. In striving for uniformity, the Commission sees no justification for departing from the detail of UPP 4 in formulating a NSW openness principle.

4.38 The Commission is of the view that an openness principle, in the form of UPP 4, should apply to both personal information and health information. There is no need for a separate health principle to be formulated addressing openness.

5. UPP 5: Use and disclosure

- Introduction
- ALRC Report 108
- Consultation paper 3
- The Commission's conclusions

INTRODUCTION

5.1 The focus of use and disclosure privacy principles is to ensure that an agency does not, broadly speaking, use or disclose personal information for a purpose other than the one for which it was collected.

Use

5.2 Under PPIPA, use of personal information is regulated by s 16 and s 17 (IPPs 9 and 10). These provide, respectively, as follows:

- An agency must not use personal information without taking reasonable steps to ensure that it is relevant, accurate, up to date, complete and not misleading.¹
- The information can only be used for the limited purpose for which it was collected, for a directly related purpose, or for a purpose for which consent has been given. It can be used without consent only if necessary to prevent or lessen a serious and imminent threat to a person's health or safety.²

5.3 Use of health information is regulated by HPP 10 under HRIPA. It is much more comprehensive than IPPs 9 and 10 and provides that, generally, an organisation must not use information for any purpose other than the one for which it was collected, or a directly related purpose if the individual would reasonably expect this. There are a number of exceptions to this general rule. Information can be used for a secondary purpose if:

- the individual has consented to the secondary use;
- there is a serious and imminent threat to life, health or safety, or a serious threat to public health or safety;
- it is reasonably necessary for management of health services, or for training or research;
- it is to find a missing person;
- it is to investigate suspected unlawful activity, unsatisfactory professional conduct or breach of discipline;

1. *Privacy and Personal Information Protection Act 1998* (NSW) s 16, IPP 9.

2. *Privacy and Personal Information Protection Act 1998* (NSW) s 17, IPP 10

- it is reasonably necessary to exercise law enforcement, complaints-handling or investigative functions; or
- it is prescribed by the regulations.

Disclosure

5.4 Disclosure of personal information is dealt with in s 18 and s 19 of PPIPA (IPPs 11 and 12). IPP 11 deals with disclosure of personal information generally and IPP 12 deals with disclosure of information “relating to an individual’s ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities” (“sensitive information”).

5.5 IPP 11 prevents disclosure to a person or body other than the individual to whom the information relates unless:

- the agency has no reason to believe that the individual would object to the third-party disclosure, and it is for a purpose directly related to the purpose for which the information was collected;³
- the individual is aware, or is reasonably likely to have been aware, that the third-party disclosure is usual practice;⁴ or
- the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health.⁵

5.6 IPP 12 is far more restrictive of disclosure of sensitive information than other personal information. Sensitive information must not be disclosed to a third party unless this is necessary to prevent a serious and imminent threat to life or health.⁶

5.7 In relation to all personal information, sensitive or otherwise, disclosure is not permitted outside NSW or to a Commonwealth agency unless there are reciprocal privacy laws in place to protect the

3. *Privacy and Personal Information Protection Act 1998* (NSW) s 18(1)(a), IPP 11(1)(a).

4. *Privacy and Personal Information Protection Act 1998* (NSW) s 18(1)(b), IPP 11(1)(b).

5. *Privacy and Personal Information Protection Act 1998* (NSW) s 18(1)(c), IPP 11(1)(c).

6. *Privacy and Personal Information Protection Act 1998* (NSW) s 19(1), IPP 12. Note that disclosure is allowed only “to prevent” a threat, not “to prevent or lessen” a threat as provided for in IPP 11.

information, or the disclosure is permitted under a privacy code of practice.⁷

5.8 Disclosure of health information is dealt with in HPP 11. The provisions of HPP 11 mirror HPP 10 (use of information).⁸ As with use of health information, disclosure of health information is only allowed for the purpose for which it was obtained, or a directly related purpose if this is reasonably envisaged by the individual to whom the information relates. There are then 11 exceptions to this principle identical to the 11 exceptions contained in HPP 10. An additional exception not present in HPP 10 allows disclosure to an immediate family member for compassionate reasons.

ALRC REPORT 108

5.9 In Report 108, the ALRC recommended that the UPPs “contain a principle called ‘Use and Disclosure’ that sets out the requirements on agencies and organisations in respect of the use and disclosure of personal information for a purpose other than the primary purpose of collection”.⁹ This reflects the approach of the NPPs in that just one principle applies to use and disclosure of personal information by Commonwealth organisations.¹⁰ It does, however, depart from the existing Principles, which regulate use and disclosure of personal information by Commonwealth agencies in two separate principles.¹¹

Model Unified Privacy Principle 5

5.10 The ALRC formulated a ‘Use and Disclosure’ principle that contains eight circumstances in which an agency or organisation can use or disclose an individual’s personal information for a purpose other than

7. *Privacy and Personal Information Protection Act 1998* (NSW) s 19(2), IPP 12. However s 19(5) may limit the operation of this, see para 11.22-11.23

8. See para 5.3.

9. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) Recommendation 25.

10. *Privacy Act 1988* (Cth) sch 3, cl 2, NPP 2.

11. *Privacy Act 1988* (Cth) s 14, Principle 10, which places limits on the use of personal information and Principle 11, which places limits on the disclosure of personal information.

the primary purpose of collection (a secondary purpose). The proposed UPP 5 provides as follows:

- 5.1 An 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:
- (a) both of the following apply:
 - (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;
 - (b) the individual has consented to the use or disclosure;
 - (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;
 - (d) the agency or 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;
 - (e) the use or disclosure is required or authorised by or under law;
 - (f) 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;
- (g) the use or disclosure is necessary for research and all of the following conditions are met:
- (i) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the use or disclosure;
 - (ii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the National Statement on Ethical Conduct in Human Research (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act;
 - (iii) the information is used or disclosed in accordance with Research Rules issued by the Privacy Commissioner; and
 - (iv) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the information in a form that would identify the individual or from which the individual would be reasonably identifiable; or
- (h) the use or disclosure is necessary for the purpose of a confidential alternative dispute resolution process.

5.2 If an agency or organisation uses or discloses personal information under paragraph 5.1(f) it must make a written note of the use or disclosure.

5.3 UPP 5.1 operates in respect of personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

Note 1: It is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 5.1 does not override any existing obligations not to disclose personal information. 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.

Note 3: Agencies and organisations also are subject to the requirements of the 'Cross-border Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.

How does UPP 5 differ from the current Commonwealth principles?

5.11 The current Principle 10, *Limits on use of personal information*, provides that:

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:
 - (a) the individual concerned has consented to use of the information for that other purpose;
 - (b) the record keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
 - (c) use of the information for that other purpose is required or authorised by or under law;
 - (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
 - (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.
2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record keeper shall

include in the record containing that information a note of that use.

5.12 The current Principle 11, *Limits on disclosure of personal information*, provides that:

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:
 - (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
 - (b) the individual concerned has consented to the disclosure;
 - (c) the record keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
 - (d) the disclosure is required or authorised by or under law; or
 - (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.
2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record keeper shall include in the record containing that information a note of the disclosure.
3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

5.13 Aside from use and disclosure being covered in two separate principles, the content of these principles is quite different from UPP 5. In summary, except in five circumstances, Principle 10 prohibits use of information for any purpose other than the one for which it was collected,

and Principle 11 prohibits disclosure to a third party. The first four exceptions, common to both principles, are where:

- the individual consents;
- a law requires or authorises the use or disclosure;
- it is for law enforcement purposes; or
- it is to prevent or lessen a serious and imminent threat to the life or health of the individual or another person.

5.14 In addition, Principle 10 makes an exception where the secondary purpose is “directly related” to the primary purpose; and Principle 11 makes an exception where the disclosure is envisaged by the individual to whom the information relates.

5.15 UPP 5 similarly allows use or disclosure for a secondary purpose if the individual consents; or a law requires or authorises the use or disclosure; or it is for law enforcement. UPP 5 is, however, far more comprehensive in relation to use for law enforcement purposes than Principles 10 and 11.

5.16 UPP 5 differs from Principles 10 and 11 in the following respects. Secondary use is allowed:

- to lessen or prevent a serious threat (imminent is not specified) to an individual’s life, health or safety; or public health or safety; or
- if related to the secondary purpose – it need only be directly related if the information is sensitive – and the individual would reasonably expect such use or disclosure.

5.17 UPP 5 allows use for a secondary purpose in three additional circumstances, not included in Principles 10 or 11. These are:

- as part of an investigation into, or reporting of, unlawful behaviour;
- where necessary for research; or
- where necessary in an alternative dispute resolution process.

5.18 The current NPP 2, although applying only to organisations and not agencies as well, is in many respects identical to UPP 5. The way in which it differs is as follows:

- NPP 2 contains clauses dealing specifically with direct marketing¹² and genetic information whereas UPP 5 does not refer to either.¹³
- The exception in NPP 2 for research, including compilation and analysis of statistics, is specifically in relation to health information and research relevant to public health or safety. Contrast UPP 5, which applies to research generally. Also, the three conditions that must be met under NPP 2.1(d) differ from the four conditions set by UPP 5.1(g). Under NPP 2.1(d), it must be impracticable to obtain consent to the use or disclosure; under UPP 5.1(g) it can be impracticable or unreasonable. Under NPP 2.1(d), the organisation must believe that there will not be further disclosure by the recipient; under UPP 5.1(g) the agency or organisation must believe that there will not be further disclosure by the recipient in a form that would or could identify the individual. Use or disclosure under NPP 2.1(d) must be in accordance with guidelines approved by the Privacy Commissioner; use or disclosure under UPP 5.1(g) must be in accordance with Research Rules issued by the Privacy Commissioner. A significant departure in UPP 5 is the inclusion of a condition that the public interest in the research activity must outweigh the public interest in the privacy of the information.
- Information can be used or disclosed under NPP 5 to prevent a serious and imminent threat to life, health or safety; whereas under UPP 5, the threat need only be serious.
- UPP 5 provides for use or disclosure of information for alternative dispute resolution whereas NPP 2 does not.

What is the rationale behind UPP 5?

One principle

5.19 In Report 108, the ALRC noted that the majority of submissions addressing this issue supported a single principle dealing with use and

12. The ALRC has recommended regulating direct marketing in a discrete privacy principle separate from the Use and Disclosure principle: ALRC Report 108, Recommendation 26-1, UPP 6. See the discussion of UPP 6 in this report.

13. The ALRC has recommended that the exception for genetic information should be moved out of the Use and Disclosure principle and be dealt with in the *Privacy (Health Information) Regulations*. ALRC Report 108 vol 2 [25.125].

disclosure.¹⁴ The Office of the Privacy Commissioner reflected many of the reasons given:¹⁵

[A single use and disclosure principle] would assist in providing a consistent approach for the handling of personal information and may go some way to alleviating the confusion that surrounds identification of whether certain activities and information handling practices are considered a “use” or a “disclosure” and which provisions should apply.¹⁶

5.20 It was also submitted that a single principle would avoid legal technical arguments associated with the confusion referred to above, significantly reduce the complexity of privacy regulation, and generally result in a more workable scheme.¹⁷

5.21 The ALRC agreed with submissions that a single principle would reduce complexity and confusion, providing it was clear that the two concepts were not thereby conflated and that agencies and organisations must continue to understand what actions constitute a use or disclosure.¹⁸ The ALRC also noted that one principle was consistent with the process of consolidating the Principles and NPPs into a single set of principles.¹⁹

Form of the principle

5.22 ***Use or disclosure for a secondary purpose.*** The majority of submissions to the ALRC’s DP 72 supported allowing use and disclosure for a secondary purpose if that was related to the primary purpose, or directly related in the case of sensitive information, and the individual would reasonably expect the agency to use or disclose the information for the secondary purpose.²⁰

5.23 Reasons for support included that this would provide more flexibility in the use of information than currently available under

14. ALRC Report 108 vol 2 [25.16]. These were submissions to Australian Law Reform Commission, *Review of Privacy Issues Paper 31 (2006)*, Questions 4-6; and Australian Law Reform Commission, *Review of Australian Privacy Law Discussion Paper 72 (2007) Proposal 22-1*.

15. See ALRC Report 108 vol 2 [25.17]-[25.18].

16. Office of the Federal Privacy Commissioner, *Submission PR 215*, 28 February 2007, quoted in ALRC Report 108 vol 2 [25.16].

17. ALRC Report 108 vol 2 [25.20].

18. ALRC Report 108 vol 2 [25.26]-[25.27].

19. ALRC Report 108 vol 2 [25.25].

20. ALRC Report 108 vol 2 [25.41].

Principle 10,²¹ while still maintaining the necessary level of privacy protection.²² It was also seen as providing a better safeguard of privacy than the current Principle 11, which allows disclosure by an agency for any unrelated purpose if the individual is informed.²³ Other submissions observed that the recommended approach has been operating effectively, “balancing privacy and operational requirements”, in the private sector.²⁴

5.24 Not all submissions agreed with the proposed form of UPP 5. The Public Interest Advocacy Centre argued that there should be a direct relationship between the secondary and primary purpose for both sensitive and non-sensitive information before use or disclosure could be allowed. It pointed out that “most Australians have a high level of concern about use of their personal information for a purpose other than the original purpose”.²⁵ The Australian Taxation Office argued that the “reasonable expectation” test would make the use principle difficult to apply.²⁶

5.25 The ALRC agreed with submissions that an approach that has worked well in the private sector should be extended to the public sector.²⁷ It concluded that the proposed two-pronged test, requiring a relationship between the secondary and primary purposes and reasonable expectation of such use or disclosure, achieves an appropriate level of privacy protection. It rejected applying the “direct relationship” test to non-sensitive information as being too onerous for organisations and having the potential to hamper legitimate health and other research.²⁸ It noted that the less stringent test was balanced by the additional protection offered by the “reasonable expectation” test.²⁹

21. This was seen as beneficial for such purposes as public health research; see CSIRO, *Submission PR 176*, 6 February 2007 and Veda Advantage, *Submission PR 163*, 31 January 2007, quoted in ALRC Report 108 vol 2 [25.37].

22. ALRC Report 108 vol 2 [25.42].

23. ALRC Report 108 vol 2 [25.42].

24. ALRC Report 108 vol 2 [25.42].

25. Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007, quoted in ALRC Report 108 vol 2 [25.46].

26. Australian Taxation Office, *Submission PR 515*, 21 December 2007, quoted in ALRC Report 108 vol 2 [25.46].

27. ALRC Report 108 vol 2 [25.49].

28. ALRC Report 108 vol 2 [25.50].

29. ALRC Report 108 vol 2 [25.50].

5.26 The ALRC was also of the view that the existing approach of Principle 11, which allows an agency to disclose personal information merely on the basis that the individual was reasonably likely to have been aware, or made aware, that information of that kind is usually disclosed to a particular entity, was unsatisfactory.³⁰ It pointed out that an individual could be told after his or her personal information had been collected that it would be disclosed to another and that the disclosure need not have anything to do with the reason for collection of the information in the first place.³¹ UPP 5 seeks to remedy this situation.

5.27 ***Threat to life, health or safety.*** The ALRC received a large number of submissions arguing that a threat to life, health or safety should not need to be both serious *and* imminent before information can be used or disclosed for a secondary purpose.³² It was argued that this hinders agencies in doing what is necessary to meet a credible threat; that they may err on the side of caution, which may not be in the best interests of those affected by the threat; and that an assessment of the seriousness and imminence of the threat may only be possible if the relevant person has the information in hand – a “Catch 22” situation.³³

5.28 Other reasons given in support of eliminating the “imminent” requirement were that the requirement: “creates additional interpretive uncertainty”; may fuel escalation of a crisis; can be difficult to establish because the information about the extent and nature of a threat is held by another party”;³⁴ makes the exception too narrow to be effective; and that its removal would make the test consistent with confidentiality provisions in social security and family assistance legislation.³⁵

5.29 Submissions opposing removal of the “imminent” requirement argued that this would lower privacy protection and deny individuals “the opportunity to exercise an appropriate degree of control over the disclosure of their personal information”.³⁶ It was also argued that “a

30. ALRC Report 108 vol 2 [25.52].

31. ALRC Report 108 vol 2 [25.52].

32. ALRC Report 108 vol 2 [25.66]. See discussion of this issue in relation to UPP 2, para 2.103-2.107 and in relation to UPP 9, para 9.38-9.40.

33. ALRC Report 108 vol 2 [25.66].

34. ALRC Report 108 vol 2 [25.67].

35. ALRC Report 108 vol 2 [25.73].

36. ALRC Report 108 vol 2 [25.77].

‘serious threat’ may create ambiguity and be difficult to apply; and ‘serious’ may not be interpreted as implying a consideration of consequence and likelihood, as suggested in DP 72”.³⁷ The Cyberspace Law and Policy Centre submitted that it would be “very dangerous” to remove the “imminent” requirement in regard to threats to public health or safety because it would open the way for claims to be made under a wide range of law enforcement and welfare programs, “including high-volume data-matching and data linkage projects”. In the Centre’s view, this was “clearly never the intention of Parliament”.³⁸

5.30 The ALRC concluded that the current requirement that the threat be not only serious but also imminent “sets a disproportionately high bar”.³⁹ This creates particular problems where there are compelling reasons to use or disclose information but it is impracticable to obtain the individual’s consent. In any case, the assessment of whether a threat is serious involves assessment of the likelihood of its materialising.⁴⁰ The ALRC pointed out that its formulation of UPP 5 contains important safeguards, in particular, the need for an agency or organisation “to have reasonable grounds for its belief that the proposed use or disclosure is essential”.⁴¹ This, it concluded, forms an appropriate balance with the public interest in averting threats to life, health and safety.⁴²

5.31 **Unlawful activity.** When the Privacy Act was amended in 2000,⁴³ a new exception to NPP 2 relating to unlawful activity was added.⁴⁴ The Explanatory Memorandum to the amending Bill stated that the exception “explicitly acknowledges that one of an organisation’s legitimate functions is to investigate, and report on, suspected unlawful activity relating to its operations”.⁴⁵ However, the wording of NPP 2.1(f) does not specifically confine the unlawful activity being investigated or reported by the organisation to activities within, or related to, the organisation.

37. ALRC Report 108 vol 2 [25.77].

38. Cyberspace Law and Policy Centre, *Submission PR 487*, 19 December 2007.

39. ALRC Report 108 vol 2 [25.83].

40. ALRC Report 108 vol 2 [25.84].

41. ALRC Report 108 vol 2 [25.86].

42. ALRC Report 108 vol 2 [25.87].

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

44. *Privacy Act 1988* (Cth) sch 3, NPP 2.1(f).

45. Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [357].

The Office of the Federal Privacy Commissioner guideline states that “ordinarily but not in all cases, the suspected unlawful activity would relate to the organisation’s operations”.⁴⁶ UPP 5.1(d) adopts NPP 2.1(f) with the wording unchanged (other than extending its application to agencies).

5.32 Submissions to the ALRC’s DP 72 did not oppose extending NPP 2.1(f) to the public sector.⁴⁷ Both the Department of Foreign Affairs and Trade and Centrelink suggested that the exception be expanded to include investigations of serious misconduct.⁴⁸ The Office of the Federal Privacy Commissioner suggested that “relevant persons or authorities” be “identified as being explicitly linked to the investigation”, otherwise the exception could be too broadly interpreted.⁴⁹ No issue was raised in DP 72 as to whether the unlawful activity should relate to the organisation’s or agency’s operations.

5.33 The ALRC did not see a need to include a reference to “serious misconduct” for two reasons.⁵⁰ First, the Office of the Federal Privacy Commissioner has interpreted “investigation” to include investigation of professional misconduct.⁵¹ Secondly, UPP 5.1(f) authorises use and disclosure by or on behalf of a law enforcement body to prevent, detect, investigate or remedy serious misconduct.

5.34 **Law enforcement.** In UPP 5.1(f), the ALRC has favoured the more comprehensive law enforcement exception of NPP 2 over Principles 10 and 11 because “[it] canvasses with greater precision the legitimate areas of law enforcement and regulation that warrant the authorisation of secondary use and disclosure of personal information” and because it promotes clarity.⁵² The ALRC also concluded that the exception should

46. Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 41.

47. ALRC Report 108 vol 2 [25.94].

48. ALRC Report 108 vol 2 [25.95].

49. Office of the Federal Privacy Commissioner, *Submission PR499*, 20 December 2007, cited in ALRC Report 108 vol 2 [25.96].

50. ALRC Report 108 vol 2 [25.98].

51. See ALRC Report 108 vol 2 [25.98]; the source of this guidance was not cited.

52. ALRC Report 108 vol 2 [25.117].

not be limited to existing investigations but should allow for enforcement agencies initiating investigations in the public interest.⁵³

5.35 **Alternative dispute resolution.** The ALRC has recommended the inclusion of a new exception relating to alternative dispute resolution (“ADR”) as this recognises the increasing significance of the role of ADR in the formal justice system as well as more broadly across commercial sectors and the community.⁵⁴ Without this exception, privacy legislation could obstruct the information exchange necessary to the resolution of disputes through ADR.

5.36 **Missing persons.** The ALRC also considered inclusion of an exception relating to missing persons but ultimately rejected this. It acknowledged that the subject raised complex issues and competing policy considerations, potentially applying to persons who in fact did not want to be found, such as in situations of family breakdown or domestic violence, and whose privacy could be seriously infringed.⁵⁵ On balance, the ALRC was of the view that where an agency or organisation had a legitimate reason to search for a missing person, the other exceptions to the use and disclosure principle should be used or a public interest determination sought.⁵⁶

CONSULTATION PAPER 3

5.37 In CP 3,⁵⁷ we raised a number of issues in relation to the operation and framework of IPPs 9 and 10 and HPP 10. The preliminary question, similarly raised by the ALRC, was whether the separate principles governing use and disclosure should be merged into one. Other issues, although specifically raised in relation to IPPs 10 and 11 and HPPs 10 and 11, are relevant to UPP 5 and are examined in paragraphs 5.38-5.57 for their bearing on UPP 5.

53. ALRC Report 108 vol 2 [25.117].

54. ALRC Report 108 vol 2 [44.23].

55. ALRC Report 108 vol 2 [25.139]-[25.140].

56. ALRC Report 108 vol 2 [25.141].

57. New South Wales Law Reform Commission, *Privacy Legislation in New South Wales* Consultation Paper 3 (2008) (“NSWLRC CP 3”).

One principle

5.38 Issue 36 asked:

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

(b) Alternatively, should the same privacy standards, and exemptions from those standards, contained in the HPPs apply equally to “use” and “disclosure” of information?⁵⁸

5.39 All submissions to CP 3 that addressed Issue 36 supported the formulation of one principle, as recommended by the ALRC.⁵⁹ The Cyberspace Law and Policy Centre submitted that the current dichotomy has led to too many examples of conduct falling between the two activities.⁶⁰ Privacy NSW observed that a single principle would significantly reduce complexity in privacy regulation.⁶¹

Form of the principle

Use or disclosure for a secondary purpose

5.40 As set out above, UPP 5.1(a) allows use and disclosure of information for a secondary purpose if: the secondary purpose is related, or directly related in the case of sensitive information, to the primary purpose; *and* the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose. IPP 11.1(a) allows information to be disclosed to a third person “if 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”. IPP 11.1(b) allows third party disclosure if the individual “is reasonably likely to have been aware, or has been made aware ... that information of that kind is usually disclosed” to the third party. No mention is made in

58. NSWLRC CP 3, Issue 36.

59. Australian Privacy Foundation, *Submission*; Cyberspace Law and Policy Centre, *Submission*; Inner City Legal Centre, *Submission*; Law Society of NSW, *Submission*; Office of the Privacy Commissioner, *Submission*.

60. Cyberspace Law and Policy Centre, *Submission*, 23.

61. Privacy NSW, *Submission*, 13.

IPP 11.1(b) of a relationship between the purpose for collection and the purpose for disclosure to another.

5.41 CP 3 raised an issue in relation to IPP 11.1(b) that should be tested against UPP 5.1(a). The Commission asked whether IPP 11.1(b)⁶² should be amended to include the phrase “and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure”.⁶³ The question relevant to UPP 5.1(a) is whether it is sufficient that the individual would reasonably expect an agency to use or disclose his or her information for the secondary purpose, or whether the agency should also demonstrate that it has no reason to believe that the individual would object to the use or disclosure.

5.42 The Australian Privacy Foundation and the Cyberspace Law and Policy Centre submitted that there should not be an exception to the ‘Use and Disclosure’ principle based solely on awareness.⁶⁴ They favoured the approach of UPP 5.1(a) pursuant to which the test is positive and objective, namely whether “the individual would reasonably expect”, rather than negative and subjective, namely that “the agency has no reason to believe the individual would object”. The NSW Department of Corrective Services did not think that the further test of the agency’s belief that the individual would not object should be added.⁶⁵ The Law Society of NSW thought it should. However, as the Australian Privacy Foundation and the Cyberspace Law and Policy Centre pointed out, there is a distinction between an individual being aware, or made aware, that information is usually discussed, and what use and disclosure could reasonably be expected. It is uncertain whether the Law Society’s response would be the same if the issue were tested against the wording of UPP 5.1(a).

62. Specifically, s 18(1)(b) of the *Privacy and Personal Information Protection Act 1998* (NSW).

63. NSWLRC CP 3 Issue 40.

64. Australian Privacy Foundation, *Submission*; Cyberspace Law and Policy Centre, *Submission*, 25.

65. NSW Department of Corrective Services, *Submission*.

Relevant purpose

5.43 Issue 37 asked:

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

5.44 The problem this issue highlighted was identifying the primary purpose of collection⁶⁶ where there have been multiple acts of collection. That is, an agency may be lawfully entitled to collect information from someone other than the individual, for a purpose different from the purpose for which the individual first provided the information. Is the “primary purpose” the purpose for which the individual gave his or her personal information or the purpose for which the agency collected it?

5.45 Submissions addressing Issue 37 all agreed that the correct interpretation is that “primary purpose” is the purpose for which the agency collected the information, whether from the individual or a third party.⁶⁷ Both the Law Society of NSW and the Cyberspace Law and Policy Centre submitted that this should be clarified in the legislation.⁶⁸ In addition, the Cyberspace Law and Policy Centre was of the view that the term “collected” could limit the operation of the principle because personal information can be created by an agency without going through a process that could be described as collection. It suggested substituting a more neutral term such as “obtained”.

Unsolicited information

5.46 Issue 38 asked whether IPPs 10 and 11, and HPPs 10 and 11, apply to unsolicited information, and, if not, whether they should apply. All submissions addressing this issue thought that the ‘Use and Disclosure’

66. IPPs 10 and 11 and HPPs 10 and 11 refer to the purpose “for which it was collected”.

67. Cyberspace Law and Policy Centre, *Submission*, 24; Law Society of NSW, *Submission*, 10; Inner City Legal Centre, *Submission*, 37.

68. Cyberspace Law and Policy Centre, *Submission*, 24.

principles should apply to unsolicited information,⁶⁹ the Law Society of NSW stating that they do not presently apply.⁷⁰

5.47 The ALRC has recommended that, if an agency receives unsolicited information, it must either destroy the information (if lawful and reasonable to do so) without using or disclosing it, or otherwise comply with all relevant UPPs as if the agency had actively collected the information.⁷¹ In CP 3, the Commission asked whether the NSW privacy principles should include a principle in terms identical, or equivalent, to the proposed UPP 2.5 (as it was then numbered in the ALRC's DP 72).⁷² The Commission discusses the proposed UPP in Chapter 2 and notes that all responses to Issue 38 supported the ALRC's approach. The Commission supports the inclusion of UPP 2.4 in privacy legislation.⁷³

Sensitive information

5.48 CP 3 raised two issues relating to the disclosure of sensitive information under PPIPA, one of which does not arise under UPP 5 because of the different approach of the Privacy Act, and one of which is relevant to UPP 5.⁷⁴

5.49 Section 19(1) of PPIPA imposes higher standards for disclosure of "personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities". The Commission describes this in CP 3 as "sensitive information", although this is not a phrase formally defined in PPIPA. CP 3 asked whether a person's criminal history and record should be included as sensitive information⁷⁵ and whether what is meant by "sexual activities" should be clarified.⁷⁶ These issues were not raised

69. Australian Privacy Foundation, *Submission*; Cyberspace Law and Policy Centre, *Submission*, 24; HIV/AIDS Legal Centre, *Submission*, 11; Inner City Legal Centre, *Submission*, 37; Law Society of NSW, *Submission*, 11; Office of the Privacy Commissioner, *Submission*, 14.

70. Law Society of NSW, *Submission*, 11.

71. ALRC Report 108 vol 1 Recommendation 21-3, UPP 2.4.

72. NSWLRC CP 3 Issue 39.

73. All responses to CP 3 supported this position: Australian Privacy Foundation, *Submission*; Cyberspace Law and Policy Centre, *Submission*, 24; Law Society of NSW, *Submission*, 11; Office of the Privacy Commissioner, *Submission*, 14.

74. NSWLRC CP 3 Issues 41 and 42.

75. NSWLRC CP 3 Issue 41.

76. NSWLRC CP 3 Issue 42.

by the ALRC in relation to the UPPs as the Privacy Act defines “sensitive information” to include an individual’s criminal record and an individual’s “sexual preferences or practices”.⁷⁷ The question that arises in relation to UPP 5 is whether “criminal history” should be included with “criminal record” as sensitive information.

5.50 Submissions addressing Issue 41 were divided in their views. The Australian Privacy Foundation, the Cyberspace Law and Policy Centre, the Inner City Legal Centre, the Law Society of NSW, Privacy NSW and the Intellectual Disability Rights Service all believed that criminal history and record should be included in the sensitive information given higher protection from disclosure.⁷⁸ The Australian Privacy Foundation and the Cyberspace Law and Policy Centre submitted that “criminal record” alone, as used in the Privacy Act, is too narrow as it can be interpreted to exclude information about arrests, charges, and so forth, that do not result in formal criminal records.⁷⁹ The phrase “criminal history” defined to include criminal records and other involvement with the criminal justice system is preferable. Privacy NSW commented that criminal record information is highly personal and has the potential to give rise to unjustified discrimination against individuals.⁸⁰

5.51 The Intellectual Disability Rights Service went further in submitting that information about the criminal history and record of a person with intellectual disability should not be disclosed unless that person has expressly consented, or it is required for legal proceedings or by law, or it is necessary to prevent a serious and imminent threat to life or health.⁸¹ The Service submitted that:

Given that people with intellectual disability are recognised under NSW criminal law statutes as having reduced culpability where certain conditions are met, it would be unfair to have their criminal

77. *Privacy Act 1988* (Cth) S 6(1).

78. Australian Privacy Foundation, *Submission*; Cyberspace Law and Policy Centre, *Submission*, 24; HIV/AIDS Legal Centre, *Submission*, 11; Inner City Legal Centre, *Submission*, 37; Law Society of NSW, *Submission*, 11; Privacy NSW, *Submission*, 14.

79. Australian Privacy Foundation, *Submission*; Cyberspace Law and Policy Centre, *Submission*, 25.

80. Privacy NSW, *Submission*, 14.

81. Intellectual Disability Rights Service, *Submission*, 6.

records disclosed on the same basis as persons without a cognitive disability ...⁸²

5.52 The Service further submitted that people with intellectual disability who have criminal convictions face discrimination and double stigmatisation, especially in the employment context.⁸³

5.53 The NSW Department of Corrective Services opposed applying special restrictions to the disclosure of a person’s criminal history and record on the basis that this would impede the Department’s role in helping an offender to adapt to community life, such as in finding appropriate employment.⁸⁴ The Department has a duty of care to ensure that individuals in the community are not unfairly placed at risk, which occasionally requires disclosure of this kind of information. If it were to be defined as “sensitive information”, the Department submitted that an exemption for law enforcement agencies, or just the Department, would be necessary.

5.54 There was unanimous support for clarifying the meaning of “sexual activities” in s 19(1) of PPIPA.⁸⁵ Adopting the phrase “sexual orientation and practices” used in the Privacy Act was favoured. However, the Department of Corrective Services submitted that it should be exempted from compliance with stricter disclosure rules as it is sometimes required to disclose information in relation to sexual offences to meet its obligations under the *Crimes (Administration of Sentences) Act 1999*. If other exceptions do not apply in the circumstances, such as there being a serious and imminent threat to the life or health of an individual or the Department having the consent of the individual, the Department submitted that it can experience delays or difficulties in meeting its obligations.⁸⁶

82. Intellectual Disability Rights Service, *Submission*, 6.

83. Intellectual Disability Rights Service, *Submission*, 6.

84. NSW Department of Corrective Services, *Submission*, 4.

85. Australian Privacy Foundation, *Submission*; Cyberspace Law and Policy Centre, *Submission*, 25; Inner City Legal Centre, *Submission*, 38; Law Society of NSW, *Submission*, 11; NSW Department of Corrective Services, *Submission*, 4.

86. NSW Department of Corrective Services, *Submission*, 4.

Investigative agencies

5.55 Issue 45 asked whether s 24 of PPIPA should be amended to exempt an agency from compliance with IPPs 10 and 11⁸⁷ when the agency is disclosing personal information to an investigative agency for the purpose of that investigative agency carrying out its complaints-handling or investigative functions.

5.56 Section 24 applies exemptions to an agency that is itself investigating a complaint. It does not apply to an agency disclosing personal information to an investigative agency. This creates problems where the investigative agency does not have coercive powers, or in situations where coercive powers are not available, and the investigative agency needs information held by the non-investigative agency to carry out its functions.

5.57 In their submissions to CP 3, the Australian Privacy Foundation and the Cyberspace Law and Policy Centre did not think s 24 should be amended.⁸⁸ The Australian Privacy Foundation submitted that there was “no justification for the wholesale exemption either of investigative agencies themselves or of ‘disclosures to investigative agencies’ from all the provisions” covered by s 24.⁸⁹ In its view, limited exemptions may be appropriate but should be narrow and contained within the applicable principle.⁹⁰ The Inner City Legal Centre, on the other hand, thought s 24 should be amended.⁹¹

THE COMMISSION’S CONCLUSIONS

One principle

5.58 In CP 3, the Commission noted that the division between “use” and “disclosure” is largely a peculiarity of Australasian privacy legislation and that, in other jurisdictions, use and disclosure are dealt with together, often under a generic expression like “processing”.⁹² The original OECD

87. The issue was also raised in relation to IPPs 2 and 3, which relate to collection requirements, and are discussed in the chapter on UPP 2.

88. Australian Privacy Foundation, *Submission*; Cyberspace Law and Policy Centre, *Submission*, 27.

89. Namely, IPPs 2, 3, 10 and 11.

90. Australian Privacy Foundation, *Submission*, 11.

91. Inner City Legal Centre, *Submission*, 39.

92. Pointed out by Crown Solicitor’s Office, NSW, *Advice*, 52.

Guidelines covered both concepts within the one “Use Limitation” principle, which applied to information “disclosed, made available or otherwise used”. Separating the concepts has its historical roots in the original privacy principles in the Privacy Act, which have since been amended. The distinction was removed in the NPPs, inserted into the Act in 2000.⁹³

5.59 Leaving the principles separate and relying on rules of statutory interpretation construing “use” and “disclosure” as having the same meaning is not an option. This construction has been rejected by the Administrative Decisions Tribunal. In *NZ v Director General, New South Wales Department of Housing*, the Tribunal held that “use” refers to “the handling of personal information within the collecting agency” and “disclosure” to “the giving of the information by the collecting agency to a person or body outside the agency”.⁹⁴ Similarly, in *JD v Department of Health*, the Appeal Panel held that “‘use’ normally bears the connotation of employing information for a purpose” and, if an agency “merely retrieves information in its possession and discloses that to an external person or body, there is no ‘use’ involved”.⁹⁵

5.60 On the other hand, the distinction between “use” and “disclosure” is not as clear-cut as the Administrative Decisions Tribunal has assumed.⁹⁶ For example, in *Director General, Department of Education and Training v MT*, the Tribunal held that s 16 of PPIPA “applies a data quality standard to all uses of personal information by an agency including conduct involving disclosure of personal information by the agency”.⁹⁷ This gives weight to Privacy NSW’s argument that having different IPPs apply to use and disclosure gives rise to technical arguments as to when processing of information involves use or disclosure.⁹⁸

5.61 The way in which PPIPA applies different standards of privacy depending on whether there is use or disclosure of the information is

93. See also the *Information Privacy Act 2002* (Vic).

94. *NZ v Director General, New South Wales Department of Housing* [2005] NSWADT 58, [69].

95. *JD v Department of Health* [2005] NSWADTAP 44, [93], [42].

96. Crown Solicitor’s Office, NSW, *Advice*, [3.41].

97. *Director General, Department of Education and Training v MT* [2005] NSWADTAP 77, [39].

98. See Crown Solicitor’s Office, NSW, *Advice*, 53.

objectionable in itself. For example, IPP 12 gives sensitive information a higher degree of protection with respect to disclosure than it receives with respect to use; an agency is required to check the accuracy of personal information before it uses it but not before it discloses it.⁹⁹

5.62 The Commission agrees with the ALRC, and with submissions both to the ALRC's Report 108 and the Commission's CP 3, that having a single principle applying to use and disclosure would remove inconsistencies, confusion and technical legal argument about which category an activity falls within. By making the legislation less complex, it is more accessible and likely to foster greater compliance.

5.63 The Commission supports UPP 5, subject to our comments below on the content of the principle.

Form of the principle

Use or disclosure for a secondary purpose

5.64 The Commission supports a privacy principle that, broadly speaking, allows information to be used or disclosed for a purpose related to the primary purpose of collection. We note that the majority of submissions to the ALRC's DP 72 were in favour of this. In our view, it is reasonable to provide agencies with this flexibility to carry out their functions, providing the exemption is counter-balanced by proper privacy protection.

5.65 In the Commission's view, the proposed UPP 5.1(a) provides a better level of privacy protection than either Principles 10 or 11, or IPP 11. Principle 10 merely states that the purpose for which the information is used must be directly related to the purpose for which the information was obtained. Principle 11 allows disclosure by an agency for any *unrelated* purpose if the individual is informed, which, in the Commission's view, is risky and difficult to justify. IPP 11 treats the exemption of UPP 5.1(a) in two parts: IPP 11.1(a) allows disclosure where it is directly related to the primary purpose and the agency has no reason to think the individual will object, with no mention of the individual's awareness or expectation; and IPP 11.1(b) allows disclosure, whether for a related or unrelated purpose, if there is the requisite awareness. Even if the individual objects to the disclosure, it is allowed under IPP 11.1(b). Furthermore, there is no condition that the individual must be aware at

99. *Privacy and Personal Information Protection Act 1998* (NSW) s 16.

the time of collection of his or her personal information. Neither provision is entirely satisfactory.

5.66 Paragraph 5.41 raises the question whether the privacy protection offered by UPP 5.1(a) could be improved. The Commission noted that three submissions responding to CP 3's Issue 40, which asked whether the condition "and the agency has no reason to believe the individual would object" should be added to IPP 11, favoured the amendment and one did not. However, the Commission also noted that IPP 11 is couched in terms of an individual's "awareness" rather than "reasonable expectation".

5.67 Nevertheless, the Commission is of the view that it is warranted to strengthen the privacy protection of UPP 5.1(a) by adding "and the agency has no reason to believe that the individual would object", given that:

- most individuals would feel uneasy about their personal information being used or disclosed for a reason other than the one for which it was collected; and
- the condition does not place any onerous burden on the agency; an agency is not required to satisfy itself that the individual does *not* object; it is only required to refrain from using or disclosing information if it has reason to believe the individual would object, that is, some evidence of objection has come to its attention or is in its possession.

5.68 Strengthening the privacy protection in this way responds to the concerns expressed to the ALRC by the Public Interest Advocacy Centre, without overly restricting an agency's functions by requiring a direct relationship between the primary and secondary purposes for all types of information, both sensitive and non-sensitive. The Commission believes that this strikes the right balance.

RECOMMENDATION 5

UPP 5.1(a) should be modified in the following way:

5.1 An agency must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection (the secondary purpose) unless:

(a) both of the following apply:

- (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 to use or disclose the information for the secondary purpose *and the agency has no reason to believe that the individual would object.*

Threat to life, health or safety

5.69 Paragraphs 5.27-5.30 canvass the arguments for and against allowing information to be used or disclosed for a secondary purpose where there is merely a “serious” threat, as opposed to a “serious *and imminent*” threat, to life, health or safety. The Commission has reached a similar conclusion as it did in relation to the collection of sensitive information in emergency situations.¹⁰⁰ That is, the Commission agrees with the ALRC that it is enough for a threat to be serious to justify using or disclosing information for a secondary purpose. First, assessing the seriousness of a risk will almost certainly involve an assessment of the likelihood, and likely timing, of its eventuating. Secondly, a threat may not necessarily be imminent but may still be of a level of seriousness that calls for use or disclosure for a secondary purpose, such as an illness or infection that may be slow in developing or have a lengthy incubation period. In any case, the concept of “imminent” is imprecise. Does it refer to an event that may occur in 24 hours? In a week? Within a month? Admittedly, a similar argument can be levelled at the concept “serious”, but the difficulty with employing the exemption is compounded by its use of the two tests. The Commission agrees with the ALRC that the requirement that a threat be both serious and imminent “sets a disproportionately high bar”.

100. See the discussion of UPP 2, para 2.103-2.107.

Unlawful activity

5.70 The Commission agrees that it is appropriate to allow both agencies and organisations to disclose information for a secondary purpose in order to investigate unlawful activity. However, we are not entirely persuaded by the ALRC’s reasons for not including in UPP 5.1(d) an exemption to investigate “serious misconduct”. Serious misconduct may not necessarily be unlawful but may warrant discipline or dismissal of an employee and may be handled within the organisation or agency. A law enforcement body may not be involved, in which case the investigation is not “by or on behalf of a law enforcement body” and does not fall within the exception of UPP 5.1(f). An agency or organisation may need to divulge certain personal information in order to obtain further information to assist it in its investigation into the misconduct. In the Commission’s view, it does not seem justified to hinder the agency or organisation in this process. We recommend including a specific reference to “serious misconduct” within UPP 5.1(d). This widening of UPP 5.1(d) is balanced by our recommendation that the sub-section be narrowed in other respects, as reasoned in the following paragraphs 5.71-5.72.

5.71 The Commission observed in paragraph 5.31 above that Parliament obviously took the view that in introducing NPP 2.1(f), on which UPP 5.1(d) is based, it was sufficient to explain that the sub-section “explicitly acknowledges an organisation’s legitimate role in investigating unlawful activity relating to its operations”¹⁰¹ without actually legislating this. We also noted that the federal Privacy Commissioner has clarified that “ordinarily but not in all cases, the suspected unlawful activity would relate to the organisation’s operations”.¹⁰²

5.72 In the Commission’s view, it is an important check on the inroads into an individual’s privacy permitted by UPP 5.1(d) that it be limited to investigations into an agency’s or organisation’s own activities. Perhaps if it merely allowed an agency or organisation to report its concerns to relevant persons or authorities, this would be more palatable. But for any agency or organisation, not being an investigative agency or organisation,

101. Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [357].

102. Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 41.

to use the exemption in UPP 5.1(d) to investigate *any* suspected unlawful activity is in our view too wide and should be explicitly controlled in the legislation, not left to guidelines or parliamentary explanations.

5.73 The Commission is of the view that it is not necessary to include within UPP 5.1(d) a non-exhaustive list of persons and authorities that may be considered “relevant” for two reasons. First, this introduces a level of detail not appropriate in what are intended to be high-level principles. Secondly, that the person or authority must be relevant, and that the use or disclosure must be necessary, provide sufficient parameters.

RECOMMENDATION 6

UPP 5.1(d) should be modified in the following way:

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.

Law enforcement

5.74 The Commission agrees with the ALRC’s formulation of UPP 5.1(f). We also agree that the exception should apply to investigations initiated in the public interest by or on behalf of an enforcement body, not just existing investigations. However, in our view, this is already implicitly allowed in the wording of UPP 5.1(f) and does not need to be enunciated.

5.75 Paragraph 5.55 canvasses the issue raised in CP 3 as to whether disclosure of information to an investigative agency should be allowed. UPP 5.1(f) allows an agency to use or disclose information if it believes this is reasonably necessary for one or more of a number of functions to be carried out by, or on behalf of, an enforcement body, including: law enforcement; protection of public revenue; processes relating to seriously improper conduct; and litigation before any court or tribunal. An enforcement body is defined in s 6 of the Privacy Act as one of 16 bodies, State or Territory authorities, or other agencies that are predominantly law enforcement or investigative bodies, but also include the Australian Crime Commission, the Australian Customs Service, and the Australian Prudential Regulation Authority.

5.76 UPP 5.1(f) appears to address the problem raised in relation to s 24 without creating “wholesale exemption” from a number of principles. For the purposes of NSW privacy legislation, “enforcement body” would, of course, need to be defined to include relevant State investigative bodies.

Relevant purpose

5.77 Paragraph 5.43 pointed to an issue raised in CP 3 not raised by the ALRC but nonetheless relevant to UPP 5. This relates to the legislative assumption contained in UPP 5 that the “primary purpose of collection” is clear and understood. In fact, where there have been multiple acts of collection, there is an ambiguity as to which is the “primary purpose of collection”. Is the “primary purpose” the purpose for which the individual gave his or her personal information or the purpose for which the agency collected it?

5.78 The unanimous view of submissions to CP 3 was that the “primary purpose of collection” is the purpose for which the agency collected the information, whether from the individual or a third party. The Commission accepts the views of the Law Society of NSW and the Cyberspace Law and Policy Centre that this should be clarified in the legislation.

RECOMMENDATION 7

“Primary purpose” in UPP 5 should be defined to mean the purpose for which the agency or organisation collected the personal information.

Sensitive information

5.79 The Commission prefers the approach of the Privacy Act over PPIPA to sensitive information. The Commonwealth Act uses the actual term “sensitive information” and then defines this in s 6, whereas the State Act refers to “personal information relating to an individual’s ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities” without defining this as sensitive information or using that term. With one modification, the Commission supports the Commonwealth definition of “sensitive information”, which is:

- (a) information or an opinion about an individual’s:
 - (i) racial or ethnic origin; or
 - (ii) political opinions; or
 - (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association; or
 - (vii) membership of a trade union; or
 - (viii) sexual preferences or practices; or
 - (ix) criminal record;
 that is also personal information; or

- (b) health information about an individual; or
- (c) genetic information about an individual that is not otherwise health information.

5.80 We recommend including both criminal history and criminal record as being sensitive information. We agree with the Australian Privacy Foundation and the Cyberspace Law and Policy Centre that “criminal record” alone is too narrow as it may exclude information about arrests, charges, and so forth, that do not result in formal criminal records. This is particularly important in relation to young offenders who may, for example, have been cautioned, which is recorded in police files but is not a “criminal record”.

5.81 The Commission is not persuaded that including criminal history in the category of information that is defined as sensitive would necessitate an exemption for law enforcement agencies, or the NSW Department of Corrective Services in particular. If the Department needs to use or disclose a person’s criminal history in its role of reintegrating an offender into community life, it can do so if this is directly related to the primary purpose of collection of the information, or if the individual consents, or if it can rely on any of the other exemptions. It is difficult to see how its role and discharge of its duties would be impeded by this standard of privacy. By contrast, an individual could easily suffer prejudice and disadvantage by unchecked disclosure of his or her criminal history.

5.82 We have considered the submission of the Intellectual Disability Rights Service regarding special treatment of information about the criminal history and record of a person with intellectual disability. However, we have concluded that this level of specificity is not appropriate for high-level uniform principles and would be more properly dealt with by Privacy Guidelines.

RECOMMENDATION 8

"Sensitive information" should be defined to mean:

- (a) information or an opinion about an individual's:
 - (i) racial or ethnic origin; or
 - (ii) political opinions; or
 - (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association, or a trade union; or
 - (vii) sexual preferences or practices; or
 - (viii) *criminal history, including criminal record*;
that is also personal information; or
- (b) health information about an individual; or
- (c) genetic information about an individual that is not otherwise health information.

6. UPP 6: Direct marketing

- What is “direct marketing”?
- Relevance for NSW
- ALRC Report 108
- The Commission’s view

WHAT IS “DIRECT MARKETING”?

6.1 “Direct marketing” is used by businesses to sell goods and services directly to consumers, bypassing wholesalers and retailers. The producer markets and promotes its goods or services to current and potential customers using conventional and/or electronic communication channels. The former can include mail-outs of advertising material (catalogues, leaflets, brochures or letters), telephone promotion and sales (telemarketing), broadcast fax, and direct-response television and radio. The latter includes web-based sales, email and SMS, as well as other emergent technologies. Direct marketing is a growing phenomenon in Australia, increasing in use at a rate of 17% per annum and now representing over 50% of all media spending.¹

6.2 Direct marketing has the potential to impinge on privacy where it utilises databases to target customers. It can involve “the establishment and maintenance of quantities of data about prospects and customers, which is exploited in order to enhance the probability of making a sale to each of them”.² Direct marketers can use many sources, including public registers such as the electoral roll, telephone directories and land title registers, to compile their lists of individuals to target,³ without an individual knowing his or her personal information is being collected for this purpose.

RELEVANCE FOR NSW

6.3 As explained in the Introduction, the Commission proposed in its CP 3⁴ that NSW legislation apply only to the handling of personal information by agencies⁵ and the ALRC made a corresponding recommendation in relation to the Privacy Act.

-
1. Nielsen Media Research, «<http://www.nielsenmedia.com.au/industry.asp?industryID=21>» at 9 February 2009.
 2. R Clarke, “Direct marketing and privacy” (version of 23 February 1998) «<http://www.rogerclarke.com/DV/DirectMkting.html>» at 9 February 2009.
 3. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) vol 2 [26.1].
 4. NSW Law Reform Commission, *Privacy Legislation in New South Wales Consultation Paper 3* (2008) (“NSWLRC CP 3”).
 5. NSWLRC CP 3 Proposal 3.

6.4 On the basis, then, that NSW privacy legislation will be changed to apply only to agencies, including State-owned corporations, the incidence in NSW of use of personal information for direct marketing is likely to be extremely small. It is difficult to call to mind many, if any, instances of agencies directly marketing their goods and services to prospective customers, and therefore difficult to envisage them doing so in the future. What is more common is for agencies to use contact details of its current customers to send material to those customers, such as other services the agency can offer, or information about prices and charges. It is arguable, in that context, that distribution of such material is performing a public service rather than acting as direct marketing. Be that as it may, use of personal information by NSW agencies for the secondary purpose of direct marketing will be relatively uncommon.

6.5 The main purpose of this chapter, therefore, is to contribute to the evaluation of the ALRC's recommendation for balancing privacy considerations and direct marketing practices. If not for the goal of national uniformity, a review of NSW legislation in isolation would probably have concluded that a separate privacy principle regulating direct marketing was not warranted.

ALRC REPORT 108

6.6 Following on from the view we hold that a separate privacy principle regulating direct marketing is not warranted in NSW, it is constructive to note the ALRC's conclusions.

6.7 The ALRC has recommended that the UPPs should regulate direct marketing in a discrete UPP, separate from the use and disclosure UPP.⁶ However, mirroring our thinking, the ALRC has concluded that this UPP should apply only to organisations.

Rationale for excluding agencies from the ambit of the direct marketing principle

6.8 The ALRC reviewed the submissions it received in response to the question whether agencies should be subject to the proposed direct marketing principle.⁷ It noted that there was some support for the

6. ALRC Report 108 vol 2 Recommendation 26-1.

7. ALRC Report 108 vol 2 [26.42]-[26.47]; See Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007) ("ALRC DP 72") Question 23-1.

application of the principle to agencies,⁸ including on the basis that this was consistent with the proposal for one unified set of principles,⁹ and an acknowledgement that “[t]here has been an increasing tendency for government agencies to use direct marketing techniques to promote government services and programs”.¹⁰

6.9 On the other hand, agencies submitted that there was a legitimate distinction to be drawn between their direct marketing activities and those of organisations.¹¹ They argued that when they contacted individuals it was only “to offer and/or promote government services” that are of benefit to the public whereas private sector enterprises “are trying to sell goods for their own commercial benefit”.¹² The Office of the Federal Privacy Commissioner (“OPC”) supported the agencies’ view, taking it one step further in arguing that it is a “legitimate function” of agencies to ensure individuals are “kept informed of policies, services and entitlements relevant to them”.¹³ Furthermore:

Permitting individuals to opt out of receiving this type of information from agencies may lessen the extent to which the community is aware of what the government is doing and what effect it may have on individuals.

Communications campaigns conducted by agencies are qualitatively different to the practice of “Direct Marketing” in the

-
8. Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Confidential, *Submission PR 535*, 21 December 2007; P Youngman, *Submission PR 394*, 7 December 2007.
 9. Law Council of Australia, *Submission PR 527*, 21 December 2007.
 10. Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007. See also Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.
 11. Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008; Australian Government Centrelink, *Submission PR 555*, 21 December 2007; Australian Government Department of Human Services, *Submission PR 541*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007.
 12. Medicare Australia, *Submission PR 534*, 21 December 2007. See also Australian Taxation Office, *Submission PR 515*, 21 December 2007; and Australian Government Department of Agriculture, Fisheries and Forestry, *Submission PR 556*, 7 January 2008.
 13. Office of the Federal Privacy Commissioner, *Submission PR 499*, 20 December 2007.

private sector, in that they are not conducted primarily to generate a benefit or advantage to the entity, but rather to promote a fully informed constituency.¹⁴

6.10 The OPC conceded that “agencies do not have, and should not have, an unfettered right to use personal information to contact individuals for any purpose unrelated to their administrative and policy responsibilities”.¹⁵ However, improper use and disclosure of personal information would be caught by UPP 5.¹⁶

6.11 The ALRC agreed with submissions that the application of a direct marketing principle to agencies “may preclude the legitimate communication of important information by agencies”.¹⁷ It concluded that the direct marketing UPP should not, therefore, apply to agencies.

A direct marketing principle to apply to organisations

6.12 The ALRC recommended that the direct marketing UPP should apply regardless of whether the organisation has collected the individual’s personal information for the primary purpose, or a secondary purpose, of direct marketing. The principle should distinguish between direct marketing to individuals who are existing customers and direct marketing to individuals who are not existing customers.¹⁸

6.13 The proposed direct marketing principle, UPP 6, provides as follows:

UPP 6. Direct Marketing (only applicable to organisations):

6.1 An organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing only where the:

-
14. Office of the Federal Privacy Commissioner, *Submission PR 499*, 20 December 2007.
 15. Office of the Federal Privacy Commissioner, *Submission PR 499*, 20 December 2007.
 16. ALRC Report 108 vol 2 [26.47].
 17. ALRC Report 108 vol 2 [26.48]. It is important to bear in mind that the ALRC reached its conclusions on the basis that “agencies” will not generally include Commonwealth, State or Territory commercial enterprises which are in competition with private sector organisations.
 18. ALRC Report 108 vol 2 Recommendation 26-1.

- (a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and
 - (b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications.
- 6.2 An organisation may use or disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing only in the following circumstances:
 - (a) either the:
 - (i) individual has consented; or
 - (ii) information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure;
 - (b) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications;
 - (c) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and
 - (d) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual's personal information.
- 6.3 In the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must:
 - (a) comply with this requirement within a reasonable period of time; and
 - (b) not charge the individual for giving effect to the request.

How does UPP 6 differ from the current Commonwealth principles?

6.14 There is presently no Principle under the Privacy Act dealing with direct marketing by agencies. There is, on the other hand, an NPP that deals with direct marketing by organisations as part of the use and disclosure principle. As set out in Chapter 5, NPP 2 prohibits use or disclosure of personal information for a secondary purpose, except in a number of specified circumstances.¹⁹ The exception that is relevant here is contained in NPP 2.1(c). NPP 2.1(c) permits use, but not disclosure, of personal information that is not sensitive information for direct marketing, providing a number of conditions are met. These are:

- it is impracticable to seek the individual's consent to the use of his or her information for direct marketing;
- the individual has not asked not to receive direct marketing communications;
- each direct marketing communication clearly notifies the individual that he or she can ask not to receive any more; and
- each direct marketing communication sets out the organisation's phone number and a business or electronic address, depending on whether the communication is written or sent electronically.

6.15 In addition, if the individual subsequently asks not to receive any further direct marketing communications, the organisation is prohibited from levying a charge on the individual for discontinuing the communications.

6.16 Aside from the specific reference to direct marketing in NPP 2.1(c), an organisation could use or disclose information for directing marketing purposes if:

- this was the primary purpose for which the information was collected;
- the secondary purpose of direct marketing is related (or directly related in the case of sensitive information) to the primary purpose of collection and the individual would reasonably expect the organisation to use or disclose the information for direct marketing purposes;²⁰ or

19. ALRC Report 108 vol 2 [26.9].

20. NPP 2.1(a).

- the individual consents to use of his or her information for direct marketing.²¹

6.17 Unlike NPP 2.1(c), UPP 6 allows both use and disclosure of information for direct marketing. The second significant departure from the existing principle is that UPP 6 distinguishes between an organisation's existing customers, and individuals who are not existing customers or who are younger than 15 years. UPP 6 applies different conditions to each circumstance.

6.18 In the first scenario, the organisation may use or disclose personal information for direct marketing where the individual would reasonably expect such use or disclosure; and the organisation provides the individual with an easy way of putting a stop to the direct marketing communications. The second scenario stipulates that the organisation must:

- have either the individual's express consent, or demonstrate that obtaining consent was impracticable and the information is not sensitive;
- give the individual notice that he or she can put a stop to the communications, and provide an easy way of doing so; and
- disclose to the individual the source of its information about the individual, if asked.

6.19 The decision to take direct marketing out of the use and disclosure principle and regulate it in a dedicated principle was to overcome an ambiguity relating to the purpose for which the information was collected.²² Under NPP 2.1(c), it is important to determine whether an organisation that collects personal information that it intends to use later for direct marketing has collected the information for the primary or secondary purpose of direct marketing. This is not always clear-cut. Furthermore, if it can be shown that the information was collected for the primary purpose of direct marketing, under NPP 2.1(c), it can be used "almost without restraint",²³ an entirely unsatisfactory situation. The problem of different consequences flowing depending on whether information has been collected for the primary or secondary purpose of

21. NPP 2.1(b).

22. ALRC Report 108 vol 2 [26.30]-[26.31].

23. ALRC Report 108 vol 2 [26.15], quoting *Law Council of Australia, Submission PR 177*, 8 February 2007.

direct marketing is eliminated by making the direct marketing rules apply regardless of the purpose for which the information was collected.²⁴

6.20 The ALRC acknowledged that the issue of direct marketing has been, and continues to be, the subject of a very strong response from stakeholders and the community generally:²⁵

On one hand, there is a strong push from consumers and consumer advocates to tighten the rules on direct marketing to make it more difficult for companies engaged in direct marketing to communicate with people in this way, particularly with respect to unsolicited direct marketing. This draws on the conceptualisation of privacy as including, at least, “the right to be let alone”.

On the other hand, business groups and others have emphasised the importance of direct marketing for the economy generally. They have also stressed that, if direct marketing is carried out appropriately, it can be of considerable assistance to consumers that receive direct marketing communications.²⁶

6.21 The ALRC has formulated UPP 6 so as to balance these competing positions.²⁷ Crucial to achieving the appropriate balance was to make the requirements that apply to direct marketing to individuals who are *not* existing customers more onerous than those applying in relation to existing customers.²⁸ This recognises that “direct marketing to existing customers is a legitimate business activity and is acceptable where it is within the reasonable expectations of such customers”.²⁹ UPP 6 also allows sensitive information to be used or disclosed for the purpose of direct marketing but only to existing customers and only where it is within the customer’s reasonable expectations.³⁰

6.22 Whether use or disclosure of information for direct marketing could be reasonably expected would depend on the level of sensitivity that attaches to the information.³¹ The ALRC concluded that the concept of reasonable expectation was “an appropriate way to anchor the

24. ALRC Report 108 vol 2 [26.16].

25. ALRC Report 108 vol 2 [26.27].

26. ALRC Report 108 vol 2 [26.27]-[26.28].

27. ALRC Report 108 vol 2 [26.29].

28. ALRC Report 108 vol 2 [26.33].

29. ALRC Report 108 vol 2 [26.67].

30. ALRC Report 108 vol 2 [26.83].

31. ALRC Report 108 vol 2 [26.83].

requirements applying in the context of existing customers” and noted that the concept is already used in the Privacy Act in relation to use and disclosure of information.³²

6.23 Resolving the question of whether an individual is an existing customer would depend on the particular circumstances and the organisation involved, but would need to be more than a one-off transaction and would involve an ongoing commercial, contractual or business relationship.³³ However, direct marketing to an existing customer need not be restricted to goods or services already purchased by the customer.³⁴

6.24 The part of UPP 6 that regulates direct marketing to individuals who are not existing customers was generally modelled on the existing requirements attaching to secondary purpose direct marketing under NPP 2.1(c). However, the ALRC was of the view that further protections were warranted in relation to the use or disclosure of sensitive information for the purpose of unsolicited direct marketing, and direct marketing to persons under 15 years. For example, the concept of “impracticability” under UPP 6 is broader, and more flexible, than that which exists currently in relation to secondary purpose direct marketing because “whether it is possible logistically to contact the relevant individuals is not a complete answer to the question of whether it is impracticable to obtain consent”.³⁵

6.25 The ALRC also considered whether UPP 6 should be formulated as an “opt-out” or “opt-in” model, that is, whether direct marketing may be permissible until such time as an individual indicates a wish not to be subjected to approaches (“opt-out”), or whether direct marketing approaches can only be made to those individuals who indicate that they are prepared to receive communications (“opt-in”). It proposed that the direct marketing principle should require organisations to present individuals with a simple means to opt out of receiving direct marketing communications.³⁶

32. ALRC Report 108 vol 2 [26.86].

33. ALRC Report 108 vol 2 [26.84]-[26.85].

34. ALRC Report 108 vol 2 [26.84].

35. ALRC Report 108 vol 2 [26.88].

36. ALRC DP 72 Proposals 23-3 and 23-4.

6.26 The majority of submissions received by the ALRC in response to this proposal were in support,³⁷ although some submissions qualified that support. For example, Optus and the Australian Direct Marketing Association argued that it would be too restrictive, and also unnecessary, to require each and every direct marketing communication, particularly to existing customers, to provide an individual with an opportunity to opt out.³⁸

6.27 The ALRC concluded that the concerns expressed by stakeholders were addressed by a principle that was media neutral and required organisations “to provide a simple and functional means by which an individual (whether or not an existing customer) may”, at any time, “advise the organisation that he or she does not wish to receive any further direct marketing communications”.³⁹

6.28 The ALRC concluded that it was legitimate to distinguish between existing and prospective customers in imposing conditions as to “the frequency with which express opportunities to opt out must be provided by organisations”.⁴⁰ Modelling the formulation of UPP 6.2(b) on NPP 2.1(c)(iv), the ALRC recommended that every direct market communication that is to an individual who is not an existing customer, or is under 15 years of age, must provide an opportunity to opt out of receiving further direct marketing communications.⁴¹ The ALRC was of the view that this requirement was “warranted by the high level of community concern about unsolicited direct marketing”.⁴² On the other hand, it was sufficient for existing customers simply to be made aware, through an organisation’s Privacy Policy, that they had the right to opt out of direct marketing communications at any time.⁴³

6.29 UPP 6 specifically regulates direct marketing to children under 15 years of age because of their greater susceptibility to commercial manipulation as compared with adults, and less developed cognitive capacity and maturity to give informed consent. It also recognises that

37. ALRC Report 108 vol 2 [26.92].

38. ALRC Report 108 vol 2 [26.96]-[26.97].

39. ALRC Report 108 vol 2 [26.99].

40. ALRC Report 108 vol 2 [26.100].

41. ALRC Report 108 vol 2 [26.100].

42. ALRC Report 108 vol 2 [26.100].

43. ALRC Report 108 vol 2 [26.100].

digital technologies (in particular, the internet, email and SMS) are increasingly being used by organisations to target children.⁴⁴ Under UPP 6, children under the age of 15 can never be treated as “existing customers”. Rather, the provisions applying to non-existing customers likewise apply to children. UPP 6.2(a) requires the organisation to obtain the child’s consent to the direct marketing, unless it is impracticable to do so and providing the information is not sensitive. This effectively means obtaining parental consent, as the ALRC has recommended that, where it is not reasonable or practicable to assess the capacity of a child under 15 to give consent, it is presumed that he or she is not capable of consenting.⁴⁵

6.30 When UPP 6.2 was proposed in DP 72, the Obesity Policy Coalition submitted that the obligations it imposed were insufficient and would “too easily allow organisations to avoid the consent requirement where ‘it is difficult to identify, locate or communicate’ with the person with parental responsibility”.⁴⁶ To meet this criticism, the ALRC has proposed that the OPC should give guidance as to how the exception would operate so as to limit organisations claiming in inappropriate circumstances that it is impracticable to obtain parental consent.⁴⁷ The ALRC concluded that this proposal, together with the conditions imposed by UPP 6 and its recommendations regarding decision-making on behalf of individuals under the age of 18, provided sufficient protection for children.⁴⁸

6.31 The provision in UPP 6.2(d) (revealing the source from which an organisation acquired an individual’s personal information) was included to “facilitate individuals being able to assert substantive, as distinct from merely formal, privacy rights with respect to direct marketing”.⁴⁹ It enables an individual who has received unsolicited marketing communications to go to the source of the contact information and take action to have his or her name removed from the data bank, or lodge a complaint if appropriate. As the OPC submitted, this “would enhance transparency in how individuals’ personal information is handled and

44. ALRC Report 108 vol 2 [26.101].

45. ALRC Report 108 Recommendation 68-1.

46. ALRC Report 108 vol 2 [26.104].

47. ALRC Report 108 vol 2 [26.106].

48. ALRC Report 108 vol 2 [26.106]-[26.108].

49. ALRC Report 108 vol 2 [26.136].

promote handling that accords with individuals' reasonable expectations".⁵⁰ The Public Interest Advocacy Centre also submitted that it would "empower individuals to take back control" of the use of their personal information, and may encourage organisations to consider carefully "whether they have a legitimate basis for collecting the personal information in the first place".⁵¹

6.32 In formulating UPP 6.2(d), the ALRC took note of submissions objecting to the requirement to reveal the source of personal information on the basis of the difficulty and expense in complying, and the fact that its terms of reference required it to consider the "desirability of minimising the regulatory burden on business in the privacy area". It therefore limited the right to ask where an organisation got its information from to individuals who are not existing customers. This recognises that there will be most concern about privacy where there is no existing business relationship between an organisation and an individual,⁵² without unduly adding to the compliance burdens faced by organisations. Another balancing factor is introduced by the proviso that an organisation need only comply with the requirement to reveal the source of its information if this is reasonable and practicable.

THE COMMISSION'S VIEW

6.33 The Commission supports inclusion in privacy legislation of a dedicated privacy principle to regulate direct marketing. Advertising and promotional material posted to an address or deposited in a letterbox can be irritating but the increasing onslaught of direct marketing via telephone, fax, internet, email and SMS can be not merely irritating but of significant concern for its privacy implications. This is particularly so when a person has never done business with the organisation sending the communication. Individuals can also find it difficult to have their details removed from a direct marketing list, once they have been included in one.

6.34 However, the Commission agrees with the ALRC that it is fair to draw a distinction between the material sent by public sector agencies and the material sent by private sector organisations. When an agency

50. ALRC Report 108 vol 2 [26.122].

51. ALRC Report 108 vol 2 [26.123].

52. ALRC Report 108 vol 2 [26.138].

engages in direct marketing it can generally be categorised as a public service, as the purpose is predominantly to keep the public informed of policies, services, charges and entitlements, whereas, when an organisation engages in direct marketing, it is to reap commercial benefits for the organisation. The Commission therefore agrees that a direct marketing principle should apply to organisations only.

6.35 The Commission also supports drawing a distinction between direct marketing to existing customers and direct marketing to individuals who are not existing customers, and regulating the latter more strictly than the former. We also particularly support the protections that are built into UPP 6 for children under 15 years. This is a vulnerable target audience for direct marketing: children's susceptibility to media manipulation, and not yet fully developed cognitive abilities, call for special treatment by the law.

7. UPP 7: Data quality

- ALRC Report 108
- Privacy legislation in NSW: Consultation Paper 3
- The Commission's conclusions

Accuracy of data in the credit reporting environment is one of the most important consumer issues when analysing potential consumer harm. The consequences of inaccurate credit reporting information are significant.¹

7.1 The impact of poor quality data is not, however, confined to the credit reporting arena. An individual's pension entitlements could be assessed erroneously; travel documents could be denied or medical conditions misdiagnosed if decisions are made based on inaccurate, outdated or incomplete information.

7.2 Ensuring that an agency or organisation does not collect, use or disclose information without first taking reasonable steps to check that the information is accurate, complete and up to date is the core of the principle on data quality. In this chapter, the Commission analyses the model data quality principle recommended by the ALRC in Report 108 and explores its suitability in the NSW context.

ALRC REPORT 108

Model Unified Privacy Principle 7

7.3 In Report 108, the ALRC recommended that the model UPPs should contain a principle called 'Data Quality' that requires an agency or organisation to take reasonable steps to ensure that the personal information it handles is of an appropriately high quality.² The ALRC believed that a single principle containing comprehensive data quality requirements would promote greater consistency, and increase public confidence, in the handling of personal information by agencies and organisations.

7.4 UPP 7 provides:

An agency or organisation must take reasonable steps to make certain that the personal information it collects, uses or discloses is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.

-
1. Galexia, "Credit Reporting Regulatory Framework: Submission to the ALRC Privacy Inquiry" (2007) http://www.galexia.com/public/research/articles/research_articles-sub02.html at 17 September 2009.
 2. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) ("ALRC Report 108") Recommendation 27-1.

7.5 UPP 7 modifies the existing data quality requirements in two significant ways. First, it applies to both public sector agencies and private sector organisations.³ Secondly, it expressly requires that the agency or organisation take reasonable steps to ensure that the personal information it collects, uses and discloses is *relevant* as well as accurate, up to date and complete.

The rationale behind Recommendation 27-1

Current Commonwealth law

7.6 In Report 108, the ALRC noted that ensuring the quality of the personal information that an agency or organisation collects, uses and discloses is one of the fundamental obligations of federal privacy laws.⁴ To this end, the *Privacy Act 1988* (Cth) contains a number of provisions intended to ensure that agencies and organisations take whatever steps are reasonable to check that the personal information they handle is accurate, up to date, complete and (in respect of agencies only) relevant.⁵

7.7 The current NPPs, which regulate how personal information is handled in private sector organisations, contain a specific principle dealing with data quality. NPP 3 provides that:

An organisation must take reasonable steps to make sure that the personal information that it collects, uses or discloses is accurate, complete and up-to-date.⁶

7.8 Under NPP 3, an organisation is required to take reasonable steps to check the information only at the time of collection, use or disclosure, and not at any other time.⁷ However, there may be other times where the

3. This is consistent with the ALRC's recommendation that a single set of privacy provisions ought generally to apply to both public sector agencies and private organisations, unless there are sound reasons to the contrary: see ALRC Report 108 vol 1 Recommendation 18-2.

4. ALRC Report 108 vol 2 [27.2].

5. *Privacy Act 1988* (Cth) s 14 Principle 3(c), Principle 8, sch 3, NPP 3. See also ALRC Report 108 vol 2 [27.2] - [27.3].

6. *Privacy Act 1988* (Cth) sch 3, NPP 3.

7. Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 43.

information needs to be corrected, for example, at the request of the individual under the access and correction principle.⁸

7.9 While there is no “stand-alone” data quality principle applying to public sector agencies in the *Privacy Act 1988* (Cth),⁹ features of data quality are present in a number of the Principles.¹⁰ Principle 3 provides that an agency must take reasonable steps to ensure that the information it asks for is: relevant for the purpose for which it is collected; up to date; and complete.¹¹ Principle 7 provides that an agency should take whatever steps as are reasonable to ensure that the personal information in its records is relevant, up to date, complete, accurate, and not misleading.¹² In addition, Principle 8 provides that an agency should not use the personal information in its records without taking reasonable steps to ensure that it is accurate, up to date and complete.¹³

7.10 The ALRC considered it anomalous that private sector organisations, but not public sector agencies, were subject to a discrete data quality principle, and, in its earlier discussion paper, proposed that a single data quality principle should apply to both public sector agencies and private organisations.¹⁴

Scope of existing data quality requirements

7.11 In formulating the model data quality principle, the ALRC took into consideration the scope of the existing requirements applying to private sector organisations and public sector agencies. The ALRC found that these differ in a number of ways. For example, while NPP 3 imposes data quality obligations at the time of collection, use and disclosure of personal information, Principles 3 and 8 impose data quality requirements only when the information is collected and used, not disclosed.¹⁵

7.12 There are also varying requirements relating to information outside the possession or control of the agency or organisation. Under NPP 3, an

8. See Chapter 9 generally.

9. *Privacy Act 1988* (Cth) s 14.

10. ALRC Report 108 vol 2 [27.4]-[27.5].

11. *Privacy Act 1988* (Cth) s 14 Principle 3(c).

12. *Privacy Act 1988* (Cth) s 14 Principle 7.

13. *Privacy Act 1988* (Cth) s 14 Principle 8.

14. ALRC DP 72 Proposal 25-1.

15. ALRC Report 108 vol 2 [27.6].

organisation must ensure that information it “collects, uses or discloses” is of a sufficiently high quality. Principle 8, on the other hand, applies more broadly to documents in an agency’s “possession or control”. Consequently, both the agency that outsources the handling of personal information to another agency, and the agency that merely holds the personal information on behalf of someone else, must comply with the data quality requirements.¹⁶

7.13 Another difference is the express requirement on public sector agencies that the information collected is relevant for the purpose for which it was collected.¹⁷ Principle 9 similarly requires that personal information be used only for “relevant purposes”.¹⁸ In contrast, there is no equivalent requirement of “relevance” in the NPPs.¹⁹

7.14 The way the data quality criteria are to be applied was also found to differ.²⁰ Agencies are required to interpret the information they collect having regard “to the purpose for which the information was collected”²¹ and “to the purpose for which the information is proposed to be used”.²² There is no comparable requirement in any of the NPPs.

Discussion Paper 72

7.15 In DP 72, the ALRC proposed that there be one common principle applicable to both the public and private sector. Merging features of the existing data quality requirements, the ALRC proposed that an agency or organisation should be required:

to take reasonable steps to make sure that personal information it collects, uses or discloses is, with reference to a purpose of collection permitted by the proposed UPPs, accurate, complete, up-to-date and relevant.²³

Submissions to the ALRC in response to DP 72

7.16 **A single discrete principle.** The majority of submissions received by the ALRC in response to DP 72 supported the proposed data quality

16. ALRC Report 108 vol 2 [27.11].

17. See Principle 3.

18. *Privacy Act 1998* (Cth) s 14, Principle 9. See also para 5.43-5.45.

19. ALRC Report 108 vol 2 [27.12].

20. ALRC Report 108 vol 2 [27.13].

21. *Privacy Act 1998* (Cth) s 14, Principle 3.

22. *Privacy Act 1998* (Cth) s 14, Principle 8.

23. ALRC DP72 Proposal 25-1.

principle,²⁴ and in particular, agreed that a single discrete data quality principle should apply equally to public sector agencies and private sector organisations.²⁵ It was agreed that a single principle would remove the present confusion caused by the different standards applicable to agencies and organisations, and would promote greater consistency, and thereby increase public confidence, in the handling of personal information by agencies and organisations.

7.17 The ALRC rejected a suggestion that the data quality and data security principles²⁶ be merged into one so that agencies and organisations would need to have reference only to the one principle dealing with the quality and security of record keeping.²⁷ The ALRC was of the view that the two were quite distinct and warranted separate principles.

7.18 **Possession or control.** The ALRC considered that the data quality requirements should only apply to information that an agency or organisation “collects, uses or discloses”. It concluded that extending the data quality requirements to information in an agency’s possession or control would place an onerous, and often unreasonable, burden on agencies that merely hold personal information on behalf of someone else.²⁸

7.19 **Relevance.** As proposed in DP 72, UPP 7 contains the added requirement that the information collected by an agency or organisation should be *relevant* for the purpose for which it is collected, used or disclosed.

7.20 Although there was broad support for adding the criterion of relevance to the data quality principle, a number of submissions were opposed to the proposal. One argument was that it was superfluous in light of the collection principle, which requires that an agency or organisation only collect information that is necessary for its purpose or function.²⁹ Another was that it would prevent agencies and organisations

24. ALRC Report 108 vol 2 [27.15].

25. ALRC Report 108 vol 2 [27.8]

26. The data security principle is discussed in Chapter 8.

27. ALRC Report 108 vol 2 [27.9]

28. ALRC Report 108 vol 2 [27.22]-[27.23].

29. See Chapter 2 generally.

from collecting personal information the relevance of which may only become apparent some time after collection.³⁰

7.21 The ALRC rejected both arguments. Rather than being inconsistent with, or redundant because of, the collection principle, the ALRC considered that requiring information to be relevant to the purpose for which it is collected, used or disclosed would complement the collection principle.³¹ It also considered it appropriate to require an agency or organisation to use or disclose only that portion of the information it holds as is relevant to that particular use or disclosure.³²

7.22 On the second point, the ALRC said that an agency or organisation that collected information that was unnecessary for one or more of its functions would be in breach of the collection principle. It was, therefore, appropriate that retaining such information should also put the agency or organisation in breach of the data quality requirements. In any case, the ALRC noted that Principle 3 already contained a relevance requirement; it was merely extending the obligation to private sector organisations.³³

7.23 **Measuring data quality.** What standard of quality will discharge the obligations under UPP 7? In DP 72, the ALRC had originally proposed that the data quality principle be interpreted having regard to “a purpose of collection permitted by the proposed UPPs”.³⁴ However, as submitted by the Cyberspace Law and Policy Centre, this standard may not be appropriate or even meaningful where the information is proposed to be used for a different (approved) purpose. Accepting this argument, the ALRC modified its original formulation so that the data quality principle be interpreted “having regard to the purpose for which it is collected, used or disclosed”.³⁵

What are “reasonable steps” to take to ensure data quality?

7.24 What would be considered reasonable for an agency or organisation to do in order to ensure the data quality of the personal information it holds depends very much on the nature of that information

30. ALRC Report 108 vol 2 [27.18]. Law enforcement and consular activities were cited as examples of situations where this may arise.

31. ALRC Report 108 vol 2 [27.24].

32. ALRC Report 108 vol 2 [27.25].

33. ALRC Report 108 vol 2 [27.27].

34. See discussion at ALRC Report 108 vol 2 [27.28].

35. ALRC Report 108 vol 2 [27.19].

and the purpose for which it is intended to be used and disclosed.³⁶ Some information is not likely to require any updating as it is not likely to change, such as a person's date of birth. Other kinds of personal information, however, do vary, and sometimes with great frequency, such as income and address details. In relation to these, it would therefore be reasonable to expect that an agency would take measures to check the information, probably with the individual concerned, and update the information if required. This would be particularly advisable where the information could be used to a person's disadvantage.³⁷ According to the Office of the Privacy Commissioner, most of the complaints it receives are about agencies using personal information that they had not first checked for accuracy.³⁸

7.25 The legal obligation to maintain data quality arises only when an agency or organisation collects, uses or discloses the information.³⁹ However, there is a concern that some organisations may interpret their obligations under the data quality principle in a way that could result in unjustifiable intrusions into an individual's privacy,⁴⁰ for example, by requesting information from a person to update their details when it is not strictly necessary to do so.

7.26 In order to respond to this concern, the ALRC considered whether UPP 7 should contain an express statement that the obligation to check the accuracy of personal information is qualified by the limitation that the organisation must take steps that are "reasonable" in the circumstances.⁴¹ As noted in the ALRC report, similar statements are provided for in OECD guidelines and in Canadian privacy laws.⁴² Principle 4.6.2 of the

36. See Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1 – 3*, 24-27; and Commonwealth, Office of the Federal Privacy Commissioner, *Private Sector Information Sheet 28 – NPP 3 Data Quality* (May 2009), 1.

37. Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1 – 3*, 25-27.

38. Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1 – 3*, 24.

39. See para 7.7-7.9.

40. Office of the Federal Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 267-8, cited in ALRC Report 108 vol 2 [27.30].

41. ALRC Report 108 vol 2 [27.30]-[27.33].

42. ALRC Report 108 vol 2 [27.31].

Personal Information Protection and Electronic Documents Act 2000 (Canada),⁴³ for example, provides:

An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

7.27 In its submission to both the ALRC and NSWLRC review, the Cyberspace Law and Policy Centre argued that there should be an express statement in the statute, or in a Note, or in the Explanatory Memorandum that, when determining what action is reasonable, agencies should give “primary regard ... to the extent to which data processing error can have detrimental consequences for the data subjects.”⁴⁴ It argued that this would ensure that agencies and organisations do not simply focus on their own needs when checking and updating personal information.

7.28 Ultimately, though, the ALRC’s preferred approach was to rely on guidelines issued by the Office of the Privacy Commissioner. These would detail the matters that an agency and organisation would need to consider when deciding what steps would be reasonable for it to take to check the accuracy of data.⁴⁵ The guidelines would undoubtedly build upon those already published by the Privacy Commissioner.⁴⁶ In its current guidelines on the Principles, for example, the Office of the Privacy Commissioner says that agencies that try to collect personal information which is irrelevant or unnecessary are likely to be intruding unreasonably on people’s privacy and could be found in breach of Principles 1 and 3.⁴⁷ In addition, in a recently published Information Sheet⁴⁸ for private organisations, the Office of the Privacy Commissioner notes that:

43. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (Canada), Principle 4.6.2.

44. Cyberspace Law and Policy Centre, *Submission to the ALRC DP 72*, 49. Cyberspace Law and Policy Centre, *Submission*.

45. ALRC Report 108 vol 2 [27.35].

46. See, for example, Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001).

47. Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1-3* (1994), 28.

48. Information Sheets are advisory only and are not legally binding.

Using personal information that is inaccurate, incomplete or out-of-date raises compliance and operational risks for businesses, and can result in adverse consequences for individuals.

At the same time, organisations need to take a balanced approach to data accuracy. For example, data accuracy should not involve unnecessary intrusion on an individual's privacy.⁴⁹

Deceased individuals

7.29 In formulating the model UPP, the ALRC also gave consideration to its application to information relating to individuals who were deceased, and to decisions made by automated means.

7.30 The ALRC acknowledged that checking information relating to a person who has since died would undoubtedly present challenges for the agency or organisation. It agreed, for example, that the information was likely to become out of date following the death of the individual, and that checking the accuracy of the data would necessarily involve contacting third parties.⁵⁰ Notwithstanding these difficulties, the ALRC recommended that the data quality principle be extended to personal information about deceased individuals. It noted that the obligations under the data quality principle are not overly onerous; they are qualified by the limitation that an agency or organisation need only take "reasonable steps" to ensure the accuracy of information relating to deceased individuals.⁵¹

7.31 Unlike the Commonwealth, NSW privacy law currently extends to the protection of personal information relating to an individual who has been dead for up to 30 years.⁵²

Automated decision-making

7.32 Agencies and organisations are increasingly making use of wholly automated systems for data processing and decision-making. As these decisions can have a significant impact on the lives of people, and because such systems are not foolproof,⁵³ many privacy advocates argue that automated decisions need to be periodically checked manually for

49. Office of the Federal Privacy Commissioner, *Private Sector Information Sheet 28 – NPP 3 Data Quality* (May 2009), 1.

50. ALRC Report 108 vol 1 [8.78].

51. ALRC Report 108 vol 1 [8.77]-[8.80].

52. *Privacy and Personal Information Protection Act 1998* (NSW) 4(3)(a).

53. ALRC Report 108 vol 1 [10.78].

accuracy and correctness. They argue that agencies and organisations should be required to perform these manual checks particularly where decisions are made that are detrimental to the individual, such as in loan or credit card applications, or access to welfare benefits.⁵⁴

7.33 The ALRC considered whether reviews of automated decisions should be mandated within UPP 7 or whether it was sufficient to rely on guidelines issued by the Office of the Privacy Commissioner. These guidelines could indicate particular times and circumstances when it is appropriate for agencies and organisations to review automated decisions.⁵⁵

7.34 The ALRC considered it unnecessary to add a further express requirement for a review of automated decisions in UPP 7, believing that the principle was framed broadly enough to achieve those outcomes.⁵⁶ Assistance and information could, instead, be provided to agencies and organisations in the way of guidelines. It noted that material is already available from the Administrative Review Council and the Australian Government Information Management Office in relation to the use of computer decision-making models in the public sector, and that such material could inform the development of guidelines by the Office of the Privacy Commissioner.⁵⁷

PRIVACY LEGISLATION IN NSW: CONSULTATION PAPER 3

Current data quality provisions

7.35 Although there is no discrete data quality principle in NSW privacy law, there are data quality requirements in the IPPs and in the HPPs.

7.36 IPP 4 and HPP 2 are expressed in the same terms. They require an agency or organisation that collects information from an individual to take reasonable steps to ensure that the information is:

- relevant to the purpose for which it is collected;
- not excessive;

54. ALRC Report 108 vol 1 [10.80]-[10.81].

55. ALRC Report 108 vol 1 [10.79].

56. ALRC Report 108 vol 1 [10.83]-[10.85].

57. ALRC Report 108 vol 1 [10.77]-[10.79].

- up to date; and
- complete.

7.37 The collection of the information must also not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.⁵⁸

7.38 IPP 9 and HPP 9 are also similarly worded. They provide that an agency or organisation that holds information must take reasonable steps to ensure that, before using it, the information is relevant, accurate, up to date, complete and not misleading.⁵⁹

Differences between the NSW provisions and UPP 7

7.39 UPP 7 requires four elements: accuracy, completeness, currency and relevance. IPP 4 and HPP 2 require these four elements but they additionally require that the information is “not excessive”. IPP 9 and HPP 9 also require the same four elements as UPP 7 but contain the added requirement that the information not be “misleading”. These differences are, arguably, semantic.

7.40 The requirement that agencies and organisations collect personal information that is “not excessive”, in the context of IPP 4 and HPP 2, would appear to mean that while the data must be complete, the agency and organisation must only gather information which is relevant to the purpose for which it is being collected. If the requirements for relevance, completeness and currency are satisfied, therefore, it is unlikely that the information collected would be considered excessive, thus suggesting that this requirement is redundant.

7.41 The same may be argued in relation to the requirement that personal information held by an agency or organisation should not be misleading. While it is possible that information that is accurate may nonetheless be misleading if it is either incomplete or irrelevant, the fact that IPPs 4 and 9, and HPPs 2 and 9 require all four elements – accuracy, completeness, currency and relevance – removes the likelihood that the information could be misleading.

58. *Privacy and Personal Information Protection Act 1998* (NSW) s 11; *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 2.

59. *Privacy and Personal Information Protection Act 1998* (NSW) s 16; *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 9.

7.42 Another difference between the NSW data quality provisions and UPP 7 is the qualification, in NSW law, that an agency or organisation “must not intrude to an unreasonable extent” in the individual’s privacy. The equivalent statement in the model UPPs is contained in the collection principle, specifically UPP 2.2. This provides that “an agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way”.⁶⁰ As the qualification relates to how agencies and organisations collect information, the Commission considers it is appropriate that it be contained in the collection principle rather than the data quality principle.⁶¹

Information collected indirectly from third parties

7.43 One issue raised in CP 3 was whether the notification and data quality requirements of PPIPA, contained in s 10⁶² and 11 respectively, apply to personal information that is not collected directly from the individual to whom the information relates.⁶³ Both of these sections expressly apply where a public sector agency “collects personal information from an individual”. It is not immediately clear whether this phrase means collected directly from the individual about whom the information relates.⁶⁴ This issue and its implications for the notification principle are explored in greater detail earlier in this report.⁶⁵ The Commission’s analysis in relation to the application of the notification

60. See para 2.4.

61. The Commission recommends that UPP 2.2 be adopted. See discussion at para 2.20-2.24.

62. Section 10 provides that before information is collected from an individual, or as soon after as is practicable, the agency must make the individual to whom the information relates aware of a number of things including: the fact and purpose of the collection, the intended recipients of the information, whether collection is required by law, rights to access and correct the information, and contact details of the collecting and holding agencies. See IPP 3 discussed at para 3.50.

63. NSW Law Reform Commission, *Privacy Legislation in New South Wales* Consultation Paper No 3 (2008) (“NSWLRC CP 3”) [6.20]. These sections refer to IPPs 4 and 3 respectively.

64. The issue does not arise in relation to the data quality requirements of IPP 9 and HPP 9. These apply to information that an agency “holds”, and therefore clearly extend to personal and health information that the agency handles, regardless of whether it was obtained directly or indirectly, and irrespective of whether the information was actively solicited or not.

65. See discussion at para 3.44-3.59.

principle to information collected indirectly from a third party applies equally in relation to the application of the data quality principle.

7.44 The Administrative Decisions Tribunal has held that s 10 and 11 are limited to personal information collected directly from the individual concerned.⁶⁶ However, there is an argument that the decision of the Tribunal in *HW v Director of Public Prosecutions (No 2)* may not be correct.⁶⁷ After considering the decision in *HW* and the opposing view, the Commission concluded, in CP 3, that both the notification and data quality principles (IPPs 3 and 4) ought to apply regardless of whether the information was collected directly from the individual concerned or indirectly from another source.⁶⁸

7.45 We also noted that this is consistent with the approach in HPP 4, which, in subclause (2) refers specifically to the situation where health information about an individual is not collected directly from that person. In those circumstances, the organisation is required to take reasonable steps to ensure that the individual is informed of the collection and made aware of matters equivalent to IPP 3.⁶⁹

7.46 The majority of submissions that addressed this issue supported extending the data quality obligations to information obtained from a third party.⁷⁰ However, the NSW Department of Corrective Services argued that it would be impractical for law enforcement agencies to comply with it, and they should therefore be exempted.⁷¹ The Crown Solicitor's Office also foresaw compliance issues.⁷²

7.47 The Commission's proposal in CP 3 that the requirements imposed by IPPs 3 and 4 should apply whether the information is collected

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

67. See discussion of the decision in *HW v The Director of Public Prosecutions (No 2)* at para 3.58.

68. NSWLRC CP 3 Proposal 10. See discussion at [6.23]-[6.25].

69. See *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 4.

70. Australian Privacy Foundation, *Submission*, whose views were endorsed by the Consumer Credit Legal Centre, Inner City Legal Centre, *Submission*, Public Interest Advocacy Centre, *Submission*, Cyberspace Law And Policy Centre, *Submission*, Office of the Privacy Commissioner, *Submission*.

71. NSW Department of Corrective Services, *Submission*.

72. Crown Solicitor's Office, *Advice*, [3.17] cited in NSWLRC CP 3 [6.22].

directly or indirectly⁷³ is also consistent with UPP 3. This provides that agencies and organisations must notify or otherwise ensure that individuals are made aware of the fact that the information has been collected; and their rights of access to, and correction of the information.⁷⁴ While it is not necessary to identify the source of the third party from whom the information was obtained, notifying the person of the matters in UPP 3 is a way of ensuring that the information is correct and consequently of complying with the data quality requirements. This rationale applies irrespective of whether information is collected directly or indirectly from the individual.⁷⁵

7.48 Chapter 3 outlines the ALRC's views and recommendations in relation to the entitlement of individuals to be notified of certain specified matters relating to the collection of their personal information regardless of whether that information was obtained directly from the individual or from a third party.⁷⁶ The Commission supports the ALRC's formulation of UPP 3 and recommends that UPP 3 be adopted in the NSW context.⁷⁷

Unsolicited information

7.49 A similar issue arises in relation to personal information that an agency takes no active steps to collect. The treatment of unsolicited information is discussed in greater detail in Chapter 2. The Commission recommends the adoption of UPP 2.5 which essentially provides that where an agency or organization receives unsolicited information, it must either destroy the information without using or disclosing it, or, if it decides to retain the unsolicited information, comply with all the relevant privacy principles as if it had actively collected the information.⁷⁸ This would include informing the individual concerned that the collection has taken place and checking the accuracy of information obtained from third parties.

73. NSWLRC CP 3 Proposal 10.

74. See discussion at para 3.1-3.2.

75. ALRC Report 108 vol 2 [23.179].

76. ALRC Report 108 vol 1 [23.90]. See also para 3.44-3.49.

77. See para 3.57.

78. See para 2.78-2.80.

THE COMMISSION'S CONCLUSIONS

Should NSW adopt UPP 7?

7.50 The Commission believes that NSW should adopt UPP 7 for a number of reasons. First, it is consistent with our broad policy aim of working, where possible, towards uniform privacy laws, or at the least, nationally consistent privacy laws.⁷⁹ Although there are some semantic differences between UPP 7 and the NSW data requirements, the Commission believes that they are essentially very similar. UPP 7 does not dilute the current obligations on agencies in NSW. There is therefore no justification for departing from our aim to achieve uniformity. Another advantage of adopting UPP 7 is that it will clarify and consolidate into the one discrete principle the slightly different obligations that are presently spread out across four principles in NSW privacy laws. This will assist record-keepers to better understand their obligations, and thus promote greater compliance with privacy laws.

Should there be a separate data quality principle regulating health information?

7.51 The Commission notes that the data quality obligations on record-keepers in relation to the collection and handling of both personal information and health information in NSW are almost identical. UPP 7, as stated above, encapsulates the essence of the current data quality obligations under HRIPA. It is a high level principle equally applicable to the collection and handling of personal information as well as health information. The Commission therefore sees no need for a separate principle regulating data quality of health information.

79. See para 0.5-0.9.

8. UPP 8: Data security

- Introduction
- What is a data security breach?
- ALRC recommendation
- Formulation of UPP 8
- Privacy legislation in NSW
- The Commission's conclusions

INTRODUCTION

8.1 Data security is fundamental to information privacy. It means protecting information from loss and unauthorised access, use, disclosure, modification and destruction. To comply with data security obligations, agencies and organisations must develop and implement systems for securely collecting and storing personal information, authorising staff to access records, ensuring the secure transfer of data, and the secure disposal of personal information when it is no longer needed or cannot lawfully be retained. Agencies and organisations must be particularly mindful of new, and increasingly sophisticated, challenges and security risks posed by threats to information systems and networks.

8.2 In this chapter, the Commission examines the model data security principle recommended by the ALRC in Report 108 and assesses its suitability for adoption in the NSW context.

WHAT IS A DATA SECURITY BREACH?

8.3 A data security breach occurs when a record containing personal information is lost or where the personal information has been subject to unauthorised access, use or disclosure.

8.4 Data security breaches do not only occur as a result of malicious external threats such as theft and computer “hacking”, although these are of increasing concern.¹ More commonly, they occur as a result of mundane mistakes and from failures to follow information handling procedures correctly, for example, by sending personal details to the wrong individual; placing sensitive personal information in recycle bins rather than shredding them; or disposing of old computers without erasing all the files contained on them. Many of the most serious privacy breaches occur from loss or theft of laptops, USB keys or files containing personal information that are not adequately secured by encryption

1. A Mosers, “CommBank cops sustained online fraud attack”, *Sydney Morning Herald*, 2 June 2009 «<http://www.smh.com.au/articles/2009/06/02/1243708447679.html>» at 2 June 2009, citing a report by the Australian Payments Clearing Association which shows a 33 per cent increase in both the volume and value of fraudulent online payments in Australia for the year ended 31 December 2008.

methods or password protected, and left unsecured at home or in cars.² Irrespective of intention, an individual's privacy is compromised wherever and however a data security breach occurs.

ALRC RECOMMENDATION

Model Unified Principle 8

8.5 In Report 108, the ALRC recommended that the model UPPs should contain a single data security principle applying to both agencies and organisations. UPP 8 is expressed in the following terms:

UPP 8. Data Security

8.1 An agency or organisation must take reasonable steps to:

- (a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure; and
- (b) 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 and retention is not required or authorised by or under law.

8.2 The requirement to destroy or render non-identifiable personal information is not 'required by law' for the purposes of the *Archives Act 1983* (Cth).

Note: Agencies and organisations also should be aware of their obligations under the data breach notification provisions.

FORMULATION OF UPP 8

Current data security obligations

8.6 UPP 8 represents a consolidation of existing data security requirements applying to agencies and organisations under the Privacy Act.³ Presently, Principle 4(a) requires an agency in possession or control of a record containing personal information to ensure that:

-
- 2. See, for example, BBC News, "NHS told to tighten data security", 25 May 2009 «http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/8066609.stm» at 31 May 2009.
 - 3. *Privacy Act 1988* (Cth) s 14 and sch 3, NPP 4.

the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse ...⁴

8.7 Principle 4(b) also requires the agency to ensure the security of a record containing personal information where that record has been provided to a third party in connection with the provision of a service to the agency. In these situations, the agency must do everything reasonably within its power to prevent unauthorised use or disclosure of the personal information contained in the record.⁵

8.8 NPP 4, applying to personal information handled by organisations, is different from Principle 4 in two respects. The first limb of the principle requires an organisation to take reasonable steps to protect the information from misuse, loss, unauthorised access, modification or disclosure.⁶ The second limb requires an organisation also “to take reasonable steps *to destroy or permanently de-identify* personal information if it is no longer needed for any purpose for which the information may be used or disclosed under [the use and disclosure principle]”.⁷ As the ALRC notes, there is no equivalent “data destruction” requirement on agencies under the Principles.⁸ The second difference between them is that, unlike Principle 4, NPP 4 does not expressly require organisations to maintain the security of records containing personal information where those records are provided to a third party.⁹

8.9 Guidelines issued by the Office of the Federal Privacy Commissioner (“OPC”) outline the kinds of measures that a record-keeper should take in order to minimise the chances of breaching its data security obligations.¹⁰ Among other things, the OPC suggests that

-
4. *Privacy Act 1988* (Cth) s 14, IPP 4(a).
 5. *Privacy Act 1988* (Cth) s 14, IPP 4(b).
 6. *Privacy Act 1988* (Cth) sch 3, NPP 4.1.
 7. *Privacy Act 1988* (Cth) sch 3, NPP 4.2.
 8. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) vol 2 [28.7].
 9. ALRC Report 108 vol 2 [28.7]. But see para 8.29.
 10. In respect of organisations, see Office of the Federal Privacy Commissioner, *Security and Personal Information*, Information Sheet 6 (2001). In relation to agencies, see Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4–7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information*

agencies and organisations should implement measures to ensure the physical security of records, such as locking documents away, installing alarm systems and preventing unauthorised entry to premises. They should also adopt measures to protect computers and networks by, for example, the use of passwords, and to secure communications by the encryption of data. In addition, agencies and organisations are advised to: limit access to personal information to authorised staff for approved purposes only; train their staff on security matters; and conduct regular audits of security systems, making sure to follow up on the outcomes of those audits.¹¹

8.10 In formulating UPP 8, the ALRC considered three issues in relation to data security provisions. They were:

- whether there was sufficient policy justification to retain separate principles for agencies and organisations, and thus depart from its umbrella policy to devise a single set of principles that would be broadly applicable to both;
- whether it was appropriate to include, in the data security principle, obligations that presently only apply to agencies or organisations; and
- the extent of the requirement on organisations to destroy or permanently de-identify personal information.

A single principle

8.11 In DP 72, the ALRC proposed that there should be a single data security principle, framed sufficiently broadly so as to respond to the different environments in which agencies and organisations operate.¹² This proposal was consistent with its overarching policy to develop a single set of principles that would apply generally to the private and public sector. Developing a single discrete principle also provided the

(1998). See also Office of the Federal Privacy Commissioner, *Guide to Handling Personal Information Breaches*, (2008).

11. Office of the Federal Privacy Commissioner, *Security and Personal Information*, Information Sheet 6 (2001), 1-4; Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4-7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 4-7.

12. Australian Law Reform Commission, *Review of Australian Privacy Law* Discussion Paper 72 (2007) (“ALRC DP 72”) Proposal 25-1.

opportunity to simplify and consolidate the current requirements, and thus resolve the gaps and inconsistencies in the current provisions.¹³ The ALRC noted that a consistent theme across submissions and consultations with various stakeholders was the importance of developing clear and broadly applicable data security provisions, particularly in light of the increasing risk of identity theft.¹⁴

8.12 Merging and consolidating the features of the current provisions, the ALRC suggested in DP 72 that the data security principle should require an agency or organisation to take reasonable steps to:

- (a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure;
- (b) destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the UPPs; and
- (c) ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.

8.13 This proposal was revised by the ALRC in its final report in view of the comments it received in submissions and in view of other relevant policy considerations. Each of the elements contained in the proposed data security principle is examined below.

Reference to data breach notification provisions

8.14 The ALRC's proposal for a single data security principle was widely supported in the submissions it received following publication of DP 72.¹⁵ However, some stakeholders suggested that UPP 8 should also contain an express reference to the data breach notification provisions,¹⁶ which the ALRC recommended be incorporated into federal privacy legislation.¹⁷ These are provisions that require agencies and organisations to notify affected individuals when a security breach has occurred resulting in the disclosure of personal information.

13. ALRC DP 72 vol 2 [25.12]-[25.13].

14. ALRC DP 72 vol 2 [25.11].

15. ALRC Report 108 vol 2 [28.9]

16. ALRC Report 108 vol 2 [28.9].

17. ALRC Report 108 vol 2 Recommendation 51-1. See Ch 51 generally.

8.15 Data breach notification provisions, in various forms, exist in the UK, Canada and in over 30 American states. They have developed out of concerns that the unauthorised disclosure of personal identifying information, as a result of a security breach, could lead to identity theft and identity fraud.¹⁸ The concern is more acute in the current digital age, which allows easier and freer movement of information. An increasing number of data security breaches,¹⁹ together with some recent high profile data security breaches, underscore these concerns.²⁰ There are presently only voluntary schemes in operation in Australia. In a general guidance that it accepts is entirely voluntary, the OPC outlines key steps and factors for agencies and organisations to consider when responding to a security breach, including whether to notify individuals who may be affected by a breach of information security safeguards.²¹

8.16 In Report 108, the ALRC conceded that there are links between data security obligations and data breach notification provisions. For example, a requirement to notify data breaches, and thus be exposed to significant damage to reputation, can act as an incentive for agencies and organisations to implement adequate security safeguards to ensure that information is secure in the first place.²² Also, evidence that an agency has implemented security measures to protect personal information may assist the agency to claim an exception to the data breach notification provision, in the event of loss or unauthorised use.²³

18. ALRC Report 108 vol 2 [51.4]-[51.7].

19. See ALRC Report 108 vol 2 [51.11]-[51.12].

20. In 2007, for example, two discs sent by the UK Revenue and Customs Department to the National Audit Office for auditing purposes went astray in the post. These discs contained the personal information of over 25 million recipients of child benefit payments, including names, addresses, national insurance numbers and bank details: see BBC News, “UK families put on fraud alert” «http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm» at 18 September 2009. See also HM Treasury, *Review of Information Security at HM Revenue and Customs*, Final Report (June 2008). There have been local incidents as well, such as the recent report of hundreds of private documents found dumped on a Sydney street: see E Jensen, “Patient’s documents found in city street”, *Sydney Morning Herald*, 25 May 2009, 5.

21. Office of the Federal Privacy Commissioner, *Guide to Handling Personal Information Breaches* (2008).

22. ALRC Report 108 vol 2 [28.12], [51.10].

23. ALRC Report 108 vol 2 [28.12].

8.17 Despite their inter-relatedness, however, the ALRC regarded it as inappropriate to incorporate the data breach notification provisions into UPP 8 because the two are quite different in terms of their objectives and operation. UPP 8 is part of a broad principles-based regulatory framework. The data breach notification provision, on the other hand, requires agencies and organisations to take particular action, namely, to notify all those who may be affected by the security breach so that they may take steps to prevent or lessen the harm that the breach could cause. The ALRC said that this is an example of rules-based regulation, and is therefore best placed in the body of the statute rather than in the principles. The ALRC did, however, agree to add a note to UPP 8 cross-referencing the data breach notification provisions.²⁴

Prevention of loss and misuse

8.18 While both Principle 4 and NPP 4 require personal information to be protected from misuse and loss, the requirements are framed slightly differently in each.²⁵ Principle 4(a) requires agencies to ensure that a record containing personal information is protected “by such security safeguards as is reasonable in the circumstances against unauthorised access, use, modification or disclosure and against other misuse”. Agencies that fail to implement adequate security measures can be held to be in breach of Principle 4 even if there has been no actual loss or unauthorised use, access or disclosure of the information.²⁶ NPP 4.1, instead, places a positive obligation on an organisation to “take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure”.

8.19 Consistent with its proposal in DP 72,²⁷ the ALRC recommended that UPP 8 should be framed in the same terms as NPP 4.1 as these criteria reflect an appropriate balance between the matters sought to be regulated under the data security principle and those that are better

24. ALRC Report 108 vol 2 [28.14].

25. ALRC Report 108 vol 2 [28.16].

26. Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4-7: Advice to Agencies about Storage and Security of Personal Information, and Access to and Correction of Personal Information* (1998), 3.

27. ALRC DP 72 Proposal 25-2.

regulated under other privacy principles, such as the use and disclosure principle.²⁸

8.20 The ALRC rejected an argument from the Cyberspace Law and Policy Centre that the proposed formulation was not broad enough and may not protect against excessive access to the information, or accidental alteration or degradation falling short of loss.²⁹ While security concerns were implicit in notions of misuse and loss, the ALRC considered that any security issues that arose in relation to access, modification or disclosure would only arise where such actions were unauthorised. These instances were more appropriately dealt with under other privacy principles.³⁰

8.21 The ALRC also rejected a suggestion that the data security principle should contain additional provisions for the security of personal information exchanged over the internet,³¹ as this was inconsistent with its policy to devise a set of technologically neutral principles capable of general application.³²

The “reasonable steps” requirement

8.22 One of the issues raised in DP 72 was the extent of the requirement on agencies and organisations to take reasonable steps to safeguard the security of personal information. In particular, the ALRC considered whether it was necessary to elaborate on the meaning of the phrase, and if so, whether such explanation should be included in the data security principle or in guidelines issued by the OPC.³³

8.23 Many stakeholders argued that there was a need for a clearer and fuller explanation of the extent of their obligations to secure personal information. While a small number thought that the explanation should be contained in the principle itself, most accepted that further guidance could be provided by the OPC.³⁴

28. ALRC Report 108 vol 2 [28.31].

29. ALRC Report 108 vol 2 [28.23]-[28.24], [28.32].

30. ALRC Report 108 vol 2 [28.32].

31. ALRC Report 108 vol 2 [28.25].

32. ALRC Report 108 vol 2 [28.33].

33. ALRC DP 72 vol 2 [25.17]-[25.18].

34. ALRC DP 72 vol 2 [25.24]-[25.25].

8.24 Consistent with its policy to devise broad, high level principles, the ALRC favoured the latter approach. In DP 72, it proposed that the OPC issue guidelines addressing matters such as:

- including terms in contracts with service providers requiring them to handle personal information consistently with the UPPs;
- taking into account recent technological developments, including relevant encryption standards; and
- training staff adequately in security procedures.³⁵

8.25 Although the proposal was widely supported in the submissions, some stakeholders suggested that the guidelines should also address:

- the physical security of information systems and computer networks;
- security developments other than encryption methods, such as access controls and audit tools; and
- the requirements to protect personal information disclosed to a contracted service provider.³⁶

8.26 The OPC was opposed to developing guidelines addressing technological developments, arguing that this required specialised levels of expertise that it did not possess.³⁷ Acknowledging these concerns, the ALRC noted that the OPC could consult with other bodies with expertise in the area.³⁸ In addition, it recommended that the OPC be given powers under the Privacy Act to establish expert panels to assist it in this endeavour.³⁹

8.27 There were also concerns that the obligations to develop and implement systems to safeguard personal information should be commensurate with the type of information held by agencies and organisations.⁴⁰ The ALRC noted that proportionality considerations were already implicit in the requirement to take “reasonable steps”. This included assessing whether a security measure is, itself, reasonable or

35. ALRC DP 72 Proposal 25-3.

36. ALRC Report 108 vol 2 [28.27].

37. ALRC Report 108 vol 2 [28.28].

38. ALRC Report 108 vol 2 [28.37].

39. ALRC Report 108 vol 2 [28.36]-[28.37].

40. ALRC Report 108 vol 2 [28.30].

whether it is an unfounded intrusion into an individual's privacy.⁴¹ The ALRC recommended that the guidance developed by the OPC should address matters such as the:

(a) factors that should be taken into account in determining what are 'reasonable steps', including: the likelihood and severity of harm threatened; the sensitivity of the information; the cost of implementation; and any privacy infringements that could result from such data security steps; and

(b) relevant security measures, including privacy-enhancing technologies such as encryption, the security of paper-based and electronic information, and organisational policies and procedures.⁴²

Disclosure of personal information to contractors

8.28 As observed above, an agency, but not an organisation, must do everything reasonably within its power to prevent any unauthorised use or disclosure of personal information that it discloses to a third party service provider when it outsources one of its functions.⁴³ One way of complying with this principle is for the agency to include privacy clauses in contracts with third party service providers which require them to comply with Principles under the Privacy Act.⁴⁴

8.29 In DP 72, the ALRC proposed to extend the requirement in Principle 4(b) to organisations.⁴⁵ The proposal was supported by a number of stakeholders, including the OPC, who had made similar recommendations earlier.⁴⁶ The ALRC believed that extending the requirement was desirable because it would clarify the scope of NPP 4.1,⁴⁷ bring the proposed UPP into line with Principle 4(b), and was consistent

41. ALRC Report 108 vol 2 [28.39]-[28.40].

42. ALRC Report 108 Recommendation 28-3.

43. *Privacy Act 1988* (Cth) s 14, Principle 4(b). See also para 8.7-8.8.

44. Office of the Federal Privacy Commissioner, *Information Sheet 14 – 2001: Privacy Obligations for Commonwealth Contracts* (2001), 7.

45. ALRC DP 72 vol 2 Proposal 25-2 and [25.14]-[25.31]. Also Australian Law Reform Commission, *Review of Privacy Issues Paper 31* (2006) Question 4-17.

46. See Office of the Federal Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Recommendations 54 and 56.

47. There is a view that NPP 4.1, when read together with guidelines on outsourcing arrangements by organisations issued by the Office of the Federal Privacy Commissioner, already requires organisations to ensure the protection of personal information disclosed to contractors: ALRC DP 72 vol 2 [25.27].

with its overall policy to remove a number of exemptions from the Privacy Act, particularly for small business.⁴⁸

8.30 However, the ALRC reconsidered the proposed UPP 8(c) in light of several factors.⁴⁹ The most significant was the impact of s 95B of the Privacy Act. This section obliges Commonwealth agencies, when entering into contracts to provide services to or on behalf of the agency, to take contractual measures requiring the contracted service provider⁵⁰ to comply with the Principles, NPPs 7 – 10 (for which there is no equivalent in the Principles) and the requirements of s 16F on direct marketing. As a result, the proposed UPP 8(c) was considered redundant in relation to agencies.

8.31 The ALRC went on to say that the proposed UPP 8(c) may also be redundant in relation to organisations, if its recommendations to remove the small business exemption⁵¹ and to change the cross border data flows principle⁵² were implemented. The combined effect of these recommendations is that contractors will generally be covered by the privacy principles. It is, therefore, unnecessary to add a specific provision in the data security principle requiring organisations to protect information disclosed to contractors.⁵³

8.32 If, however, the recommendations are not implemented, the ALRC suggested that a specific requirement for an organisation to take steps to ensure the protection of personal information disclosed to a contractor should be included in the data security principle, as proposed in DP 72, or be a specific provision in the Privacy Act, along the same lines as s 95B.⁵⁴

48. ALRC DP 72 vol 2 [25.26]-[25.29]. Presently, businesses with an annual turnover of less than \$3m are not covered by the *Privacy Act 1988* (Cth) s 6D.

49. ALRC Report 108 vol 2 [28.50].

50. A contracted service provider, for a government contract, is defined as an organisation that is a party to the government contract, or a subcontractor: *Privacy Act 1988* (Cth) s 6.

51. ALRC Report 108 Recommendation 39-1.

52. These are discussed at para 11.57-11.58.

53. ALRC Report 108 vol 2 [28.51].

54. ALRC Report 108 vol 2 [28.52].

Destruction and retention of personal information

8.33 Currently, organisations, but not federal public sector agencies,⁵⁵ are required to take reasonable steps to destroy or permanently de-identify personal information where it is no longer required for any permitted purpose.⁵⁶ As the ALRC observed, a data destruction requirement is a simple and effective way of ensuring that personal information that is no longer needed is not later misused or subject to unauthorised disclosure.⁵⁷

8.34 Counterbalancing these data destruction provisions are provisions in other privacy laws that require agencies and organisations to do the exact opposite, namely to *retain* information. One area in which this is commonly the case is in relation to health care information and research. A person's health and genetic information, for example, can inform that person's future care or emergency treatment, or be useful for research purposes. For this reason, health privacy law often requires health care providers to retain health information about an individual for minimum periods of time, and to follow specific procedures when records are transferred to other health care providers.⁵⁸

8.35 Public sector archives legislation is another area where agencies are required to retain information. The *Archives Act 1983* (Cth), for example, prohibits the destruction of Commonwealth records without the permission of the National Archives of Australia unless destruction is "required by law" or is consistent with "normal administrative practice".⁵⁹ Similar laws apply in respect of NSW agencies, as discussed below.⁶⁰

55. But see *Privacy Act 1988* (Cth) s 18F which requires credit providers and credit reporting agencies to dispose of certain personal information after certain timeframes.

56. In relation to a permitted purpose, see the use and disclosure principle, discussed at para 2.5-2.13.

57. ALRC Report 108 vol 2 [28.53].

58. For example, noting the name of the provider to whom the information is sent, the address at which the information was sent, and the date that it was sent: see, for instance, *Health Records and Information Privacy Act 2002* (NSW) s 25 discussed at para 8.52. See also *Health Records Act 2001* (Vic) sch 1, Health Privacy Principles 4.2, 4.3.

59. *Archives Act 1983* (Cth) s 24 discussed in ALRC Report 108 vol 2 [28.57].

60. See para 8.60-8.63.

8.36 A number of issues arose in the ALRC’s review of the data destruction and retention requirements under the Privacy Act. These were:

- the terminology used in the legislation for data destruction;
- specifying the manner of destroying information or rendering it non-identifiable;
- extending the data destruction requirement to agencies;
- permitted reasons for retaining personal information; and
- whether there should be a general right to request data destruction.

Terminology

8.37 The ALRC noted that the term “permanently de-identify” under the Privacy Act was considered ambiguous by stakeholders, and seemed to connote that the person whose data had been “de-identified” could later be re-identified.⁶¹ For example, blacking out a customer’s name from a file (once the individual ceased to be a customer) could satisfy the requirement to “de-identify” a record. However, this may not prevent the person from later being re-identified by matching the remaining information with other information that was publicly available.⁶²

8.38 The term “render non-identifiable”, on the other hand, makes it clear that additional steps are required to prevent future re-identification of data. The ALRC preferred this term and accordingly recommended that the legislation be rephrased.⁶³

How should information be destroyed or rendered non-identifiable?

8.39 The ALRC observed that requirements to destroy, or render non-identifiable, personal information caused considerable confusion among agencies and organisations.⁶⁴ In particular, agencies and organisations were not sure in what circumstances it was appropriate to destroy information as opposed to taking steps to render it non-identifiable. They were also not clear as to the precise methods required to accomplish either task.

61. ALRC Report 108 vol 2 [28.61].

62. ALRC Report 108 vol 2 [28.64].

63. ALRC Report 108 vol 2 [28.63].

64. ALRC Report 108 vol 2 [28.71].

8.40 Acknowledging that it is not always clear when the data destruction requirement applies, the ALRC recommended that the OPC should publish guidelines outlining the responsibilities that agencies and organisations have under the data security principle, including guidelines on when it is appropriate to destroy, or render non-identifiable, personal information.⁶⁵

8.41 The ALRC also recommended that the OPC develop and publish guidelines addressing the precise manner by which personal information, held in both paper-based records and in various electronic formats, should be destroyed or rendered non-identifiable. For example, this may include developing policies and procedures for burning, pulverising or shredding personal information held in paper-based records, or the destruction or erasure of electronic media containing personal information, so that the information can no longer be read or reconstituted. The ALRC suggested that, in developing such guidelines, it may be useful for the OPC to refer to relevant industry standards on the destruction of personal information.⁶⁶

Extending the data destruction requirement to agencies

8.42 The ALRC considered it anomalous that the data destruction requirement did not also apply to agencies under the Privacy Act. It noted that similar data destruction requirements do apply to public sector agencies elsewhere in Australia,⁶⁷ including NSW,⁶⁸ and in some overseas jurisdictions.⁶⁹ Accordingly, the ALRC proposed, in DP 72, to extend the data destruction requirement to agencies.⁷⁰

8.43 Although the proposal was generally supported across the private and public sector, there was some concern about the compatibility of the data destruction requirement with other laws, such as archives legislation and relevant provisions under an agency's enabling legislation, which

65. ALRC Report 108 vol 2 [28.71].

66. ALRC Report 108 vol 2 [28.71].

67. See for example, *Information Privacy Act 2000* (Vic) sch 1, IPP 4.2; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 4(2); and *Information Act 2002* (NT) sch 2, IPP 4.2.

68. *Privacy and Personal Information Protection Act 1998* (NSW) s 12 (IPP 5) discussed at para 8.50.

69. See for example, *Privacy Act* RS 1985, c P-21 (Canada) s 6(3) and *Federal Data Protection Act 1990* (Germany) s 20(2) cited in ALRC Report 108 vol 2 [28.55].

70. ALRC DP 72 Proposal 25-4.

require agencies to retain information.⁷¹ There was also concern that destroying or de-identifying personal information may have a detrimental impact. For example, PIAC submitted that it could not seek compensation for its indigenous clients under the “Stolen Wages” project if the claimants’ personal information had been destroyed or rendered non-identifiable.⁷² The ALRC noted other Australian and international examples where the retention of records containing personal information was helpful many years later including the use of adoption, immigration and social welfare records to help reunite child migrants with family members.⁷³

8.44 As data destruction requirements provide an important layer of privacy protection by preventing future misuse of, or unauthorised access to, personal information that is no longer needed for a lawful purpose, the ALRC believed there were compelling reasons to extend the requirement to agencies.⁷⁴ However, noting the concerns about the potential conflict with other laws, the ALRC considered a number of exceptions that would allow agencies to retain personal information, as discussed below.⁷⁵

Permitted reasons for retaining personal information

8.45 According to the ALRC, the area of data security “illustrates how it is sometimes necessary to provide differing requirements in differing circumstances.”⁷⁶ While it accepted that an individual’s privacy is best protected by requiring record-keepers to destroy or render non-identifiable personal information that is no longer needed, it also recognised that there are some circumstances where agencies and organisations need to retain personal information, and that this should be reflected in the UPP.⁷⁷ These circumstances were essentially where the information continued to be needed for a permitted purpose, and where other laws specifically required the information to be retained.

71. ALRC Report 108 vol 2 [28.74]-[28.75].

72. ALRC Report 108 vol 2 [28.77].

73. ALRC Report 108 vol 2 [28.76].

74. ALRC Report 108 vol 2 [28.79], Recommendation 28-4.

75. ALRC Report 108 vol 2 [28.80].

76. ALRC DP 72 vol 2 [25.39].

77. ALRC Report 108 vol 2 [28.87]-[28.89].

8.46 The ALRC consequently recommended that UPP 8 should require an agency or organisation to destroy or render non-identifiable personal information where:

- the information was no longer needed for a permitted purpose under the UPPs; and
- retention was not required or authorised by or under law.⁷⁸

8.47 The first of these two limbs reflects the existing requirements under NPP 4. The second “required or authorised by law” exception is principally concerned with resolving conflicting requirements under archives legislation. It also addresses concerns about the potential for a data destruction requirement to conflict with a relevant requirement under an agency’s enabling legislation; and the need for an agency or organisation to retain personal information in the event of future litigation.⁷⁹ A similar exception exists under NSW data security provisions,⁸⁰ discussed below.⁸¹

8.48 The ALRC noted that there remained some ambiguity between the data destruction requirement under UPP 8 and s 24(2) of the *Archives Act 1983* (Cth), which provides an exception from the requirement not to destroy, or otherwise dispose of, a Commonwealth record where destruction is “required by law”. It is not clear whether the requirement to destroy or render non-identifiable personal information under the Privacy Act would come within this exception. To resolve this uncertainty, and to make it clear that the obligations under archives legislation take precedence over the data destruction requirements of the data security principle, the ALRC recommended that UPP 8 should also provide that the obligation to destroy or render non-identifiable personal

78 ALRC Report 108 vol 2 Recommendation 28-4.

79 ALRC Report 108 vol 2 [28.89].

80. See *Privacy and Personal Information Protection Act 1998* (NSW) s 12 and *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 5(2). See also s 25 of PPIPA which provides generally that it is an exception to various IPPs under the Act if an agency is “lawfully authorised or required not to comply with the principle concerned”, or “non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law”.

81. See para 8.51.

information is not “required by law” for the purposes of the *Archives Act 1983* (Cth).⁸²

Should individuals have the right to request that their personal information be destroyed

8.49 The ALRC also considered whether individuals should have a general right to request that their personal information be destroyed.⁸³ A large number of submissions were opposed to the suggestion on various grounds, including that it was too blunt an instrument and that adequate redress could alternatively be provided under the access and correction principle.⁸⁴ The ALRC agreed that it was not appropriate to give individuals a general right to require agencies and organisations to destroy their personal information.⁸⁵

PRIVACY LEGISLATION IN NSW

Current data security provisions

8.50 The data security obligations on NSW agencies are contained in IPP 5 of PPIPA.⁸⁶ It provides that a public sector agency that holds personal information must:

- not keep the information for any longer than is necessary;
- dispose of the information securely and in accordance with any requirements for the retention and disposal of personal information;
- take such security safeguards as are reasonable to protect the information against loss, unauthorised access, use, modification or disclosure, and against all other misuse; and
- where it is necessary for the information to be given to a person in connection with the provision of a service to the agency, take whatever steps as are reasonable and within its power to prevent unauthorised use or disclosure of the information.

82. ALRC Report 108 vol 2 [28.90]-[28.91].

83. ALRC DP 72 vol 2 [25.68]-[25.76]; ALRC Report 108 vol 2 [28.94]-[28.96].

84. ALRC Report 108 vol 2 [28.95].

85. ALRC Report 108 vol 2 [28.96].

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

8.51 HRIPA contains almost identical data security provisions in relation to health information.⁸⁷ However, an organisation is not required to comply with these obligations if:

- it is lawfully authorised or required not to comply with it, or
- it is otherwise permitted under an Act or any other law, including the *State Records Act 1998* (NSW), not to comply with HPP 5(1).⁸⁸

Additional security and retention obligations on private health service providers

8.52 Additional data security and retention requirements apply to private health service providers. Section 25 of HRIPA provides that a private health service provider:

- must keep an individual's health information for seven years from the individual's last visit, or until the individual is 25 years old where the health information was collected when the person was under 18 years;
- who deletes or disposes of health information must keep a record⁸⁹ of the name of the individual to whom the health information related, the period covered by it, and the date on which it was deleted or disposed of; and
- who transfers health information to another organisation and does not continue to hold a record of that information must keep a record of the name and address of the organisation to whom, or to which, it was transferred.

8.53 None of these provisions authorise a health service provider to delete or otherwise dispose of an individual's health information contrary to other laws, including Commonwealth statutes.⁹⁰

NSWLRC Consultation Paper 3

8.54 In CP 3, two specific issues arose in relation to the current data security provisions under PPIPA and HRIPA. Briefly, these were:

87. *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 5(1).

88. *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 5(2).

89. Section 25(4) provides that a record may be kept in electronic form provided it is capable of being printed.

90. *Health Records and Information Privacy Act 2002* (NSW) s 25(5).

- whether the current provisions require agencies and health service providers to ensure the secure *collection* of personal information; and
- the relationship between s 12(a) of PPIPA, which requires agencies to dispose of personal information once it is no longer needed, and the State Records Act, which prohibits agencies from disposing of State records.

8.55 Another issue raised in CP 3, concerned the appropriateness and adequacy of current obligations on agencies to ensure the security of personal information disclosed to third party contractors. The recommendation of the ALRC to abandon a similar requirement in its final formulation of UPP 8 raises particular concerns, discussed below.

Secure collection of information

8.56 The increasing use of electronic collection of information, via email and the internet, poses new challenges for the protection of personal information. One way of responding to this challenge is to require agencies to provide secure websites and to implement measures to limit access to electronic collection points by others.⁹¹ While developing and implementing such measures is generally now regarded as a matter of good business practice, and the community commonly expects it,⁹² there is no express requirement on agencies to ensure the secure collection of information. Nor is it clear that the obligation to ensure the security of information “held”⁹³ by a record-keeper extends to the collection of information prior to it being “held” in a record of some form.⁹⁴ For this reason, the Commission proposed, in CP 3, that IPP 5 and HPP 5 should

91. NSW Law Reform Commission, *Privacy Legislation in New South Wales* Consultation Paper No 3 (2008) (“NSWLRC CP 3”) [6.30].

92. Inner City Legal Centre, *Submission*.

93. Defined as personal information that is in the “possession or control” of an agency, or an employee or person engaged by the agency, or held in a State record: *Privacy and Personal Information Protection Act 1998* (NSW) s 4(4).

94. For example, in *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192, the Court of Appeal said that it was possible to distinguish a separate legislative regime for “collection” from that for “holding and disclosure”. However, it considered it more likely that the scope of personal information to which the principles applied was the same for the principles relating to collection as for those relating to holding and disclosure: [33]-[34] (Spigelman CJ with whom Tobias JA and Brownie AJA agreed).

be amended to include an express requirement for the secure collection of information.⁹⁵

8.57 This proposal was widely supported in submissions received by the Commission.⁹⁶ It was agreed that this would fill an obvious gap in the present scope of the security principle,⁹⁷ and was consistent with the goal of ensuring the security of all personal information handled by an agency or organisation.⁹⁸

8.58 The Commission notes that UPP 8 similarly applies to information that an agency or organisation “holds”.⁹⁹ Yet the data security obligation extends to the collection of personal information by reason of the fact that the privacy principles under the Privacy Act expressly apply to personal information that is held, or collected for inclusion, in a record (or generally available publication).¹⁰⁰ UPP 8, therefore, applies to personal information that is in the process of being collected, provided it is intended to be subsequently included in a record. There is no equivalent provision in PPIPA.

8.59 In the Commission’s view, the adoption of UPP 8 in NSW will not ameliorate the gap in coverage of the data security principle unless a provision equivalent to s 16B(1) of the Privacy Act is inserted into PPIPA, as the NSW Court of Appeal has previously suggested.¹⁰¹ This is a matter that goes to the heart of how personal information is defined under the Act, and, therefore, to what personal information the principles should apply. Although these are not matters that the Commission deals with specifically in this report,¹⁰² it warrants consideration here because it clearly affects the efficacy of UPP 8 in the NSW context. Subject, then, to a more detailed examination of the substantive provisions of PPIPA, which the Commission leaves for a subsequent report, the Commission

95. NSWLRC CP 3 Proposal 12.

96. Privacy NSW, *Submission*, Australian Privacy Foundation, *Submission*, Consumer Credit Legal Centre, *Submission*, NSW FOI Privacy Practitioners Network, *Submission*, Cyberspace Law and Policy Centre, *Submission*.

97. Cyberspace Law and Policy Centre, *Submission*.

98. Public Interest Advocacy Centre, *Submission*.

99. UPP 8 adopts the terminology used in NPP 4 rather than that used in Principle 4. See para 8.18-8.21.

100. *Privacy Act 1988* (Cth) s 16B. See also ALRC Report 108 vol 1 [6.123].

101. *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192 (Spigelman CJ).

102. See para 0.19-0.20.

recommends that consideration be given to amending PPIPA to make it clear that the privacy principles apply to personal information that is held, or collected for inclusion, in a record or generally available publication.

RECOMMENDATION 9

The *Privacy and Personal Information Protection Act 1998* (NSW) should be amended to provide that the privacy principles apply to personal information held, or collected for inclusion, in a record or generally available publication.

Interaction between IPP 5 and the State Records Act

8.60 Agencies face conflicting obligations under the data security principle and the *State Records Act 1998* (“State Records Act”), which prohibits a person from abandoning or disposing of a State record¹⁰³ and from damaging or altering a State record,¹⁰⁴ except in certain circumstances.¹⁰⁵ Section 21 of the State Records Act prevails over provisions of earlier Acts¹⁰⁶ and over provisions of later Acts unless they specifically provide otherwise.¹⁰⁷ The provisions of PPIPA are, consequently, to be read subject to the State Records Act unless they specifically provide otherwise.¹⁰⁸ This means that PPIPA cannot authorise an agency to destroy or dispose of personal information.¹⁰⁹ In CP 3, the Commission asked whether s 12 of PPIPA should be amended to provide that it takes effect despite the provisions of the State Records Act.¹¹⁰

8.61 The State Records Office submitted that IPP 5 should not override the retention requirements under Part 3 of the State Records Act designed to protect State records.¹¹¹ It argued that much of the State’s rich heritage

103. *State Records Act 1998* (NSW) s 21(1)(a).

104. *State Records Act 1998* (NSW) s 21(1)(d).

105. The exceptions include anything done in accordance with normal administrative practice, or anything that is authorised or required to be done under any other Act, as prescribed under the regulations: *State Records Act 1998* (NSW) s 21(2)(a), (b).

106. *State Records Act 1998* (NSW) s 21(6).

107. *State Records Act 1998* (NSW) s 21(7).

108. See, for example, s 15(4) which expressly provides that s 15, or any related provision of a privacy code of practice, applies despite s 21 of the State Records Act.

109. See NSW Crown Solicitor’s Office, *Advice*.

110. NSWLRC CP 3 Issue 68.

111. NSW State Records Office, *Submission*.

and research resources, contained in the archives collection, derived from important official records, some of which also contained personal information. According to the State Records Office, inserting a provision in PIPPA to the effect of overriding s 21 of the State Records Act would have a detrimental impact on protecting the State's historical record, with little commensurate gain in terms of improving privacy of personal information.¹¹² Privacy NSW agreed that IPP 5 should not override the State Records Act.¹¹³

8.62 The Commission also agrees that some records, particularly those having historical or research value, ought to be retained. We believe this should be the case even if those records also contain personal information about an individual that the agency no longer needs for a purpose for which the information was collected. The Commission notes that this policy is consistent with HPP 5(2), which exempts an organisation from complying with HPP 5 where:

- it is lawfully authorised or required not to comply with it; or
- non-compliance is permitted (or implied or reasonably contemplated) under an Act or any other law (including the State Records Act).

8.63 It is also consistent with the ALRC's view, reflected in UPP 8, that the obligation to destroy, or render non-identifiable, personal information should be subject to other specific laws, such as archiving legislation, that require or authorise the retention of certain information.¹¹⁴ Adopting UPP 8 would, accordingly, make it clear that an agency's responsibilities under the State Records Act take precedence over any data destruction obligations under the data security principle.

Protecting information disclosed to contractors

8.64 IPP 5(d) requires NSW agencies to take reasonable steps to ensure that any personal information that is disclosed to a third party, in connection with the provision of a service to the agency, is protected from unauthorised use and disclosure.¹¹⁵ A similar requirement is imposed in relation to health information under HPP 5(1)(d).

112. NSW State Records Office, *Submission*.

113. Privacy NSW, *Submission*.

114. See para 8.45-8.48.

115. *Privacy and Personal Information Protection Act 1998* (NSW) s 12(d).

8.65 If UPP 8 is adopted in NSW in its present form, this requirement would no longer exist. As discussed above, the ALRC considered the requirement to be redundant in so far as it relates to federal public sector agencies because of the effect of s 95B of the Privacy Act, which already requires Commonwealth agencies to impose contractual obligations on third party contractors to comply with the Principles.¹¹⁶

8.66 However, there is no similar obligation on NSW public sector agencies in PPIPA. Indeed, as PPIPA does not apply directly to organisations contracted by an agency under outsourcing arrangements, the privacy principles must be imposed on contracted service providers by way of contract. While it is generally acknowledged to be good practice to include model privacy clauses in government contracts, not all agencies do so, nor are they obliged to under statute.

8.67 This gap in the legislation has been a longstanding source of concern, particularly in view of the increasing number of services and functions, once performed by public sector agencies, now being outsourced to private service providers, at both local and State levels of government. There have, consequently, been previous recommendations to amend PPIPA to require agencies to include terms in contracts with service providers requiring them to comply with the privacy principles,¹¹⁷ as is the case at both the Commonwealth level,¹¹⁸ and in Victoria.¹¹⁹

8.68 In CP 3, the Commission proposed that PPIPA be amended to provide that, where a NSW public sector agency contracts with another (non-government) organisation to provide services for, or on behalf of, the agency, the non-government organisation should be contractually obliged to comply with the IPPs and any applicable code of practice in the same way as if the public sector agency itself were providing the services.¹²⁰

8.69 This proposal was strongly endorsed in the submissions received in response to CP 3.¹²¹ The Cyberspace Law and Policy Centre submitted

116 See para 8.30.

117. NSW Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, Recommendation 13.

118. Privacy Act s 95B. See discussion at para 8.30.

119. *Information Privacy Act 2000* (Vic) s 17.

120. NSWLRC CP 3 Proposal 7.

121. Cyberspace Law and Policy Centre, *Submission; Privacy NSW, Submission*.

further that the present system of liability under s 4(4) of PPIPA should also be retained. Under s 4(4), liability for a breach of a provision of the Act by the contracted service provider rests with the agency that contracted out the services. This acts as an incentive for the agency to negotiate privacy clauses in the contract so that it can seek to be indemnified for any damages arising from a breach of the Act by the contracted service provider.

8.70 The issue for the Commission is whether UPP 8 should be adopted in NSW in light of what was discussed and proposed in CP 3, and the feedback that we subsequently received. In the Commission's view, UPP 8 should not be adopted in NSW in its present form because it removes an essential and presently single requirement on agencies to ensure the security of personal information disclosed to third party contractors, thereby reducing the current level of privacy protection.

8.71 The Commission notes that there is some opposition to the ALRC's final formulation of UPP 8 in so far as it relates to removing the obligations to ensure the security of information disclosed to contracted third parties. The Cyberspace Law and Policy Centre believes the requirement, as proposed in DP 72,¹²² should be reinstated and apply more broadly.¹²³ It argues that the requirement to impose contractual obligations on service providers under outsourcing arrangements should be clearly stated in the principle itself. It also argues that compliance by third party contractors should not be limited to the use and disclosure principle only; they should be bound to comply with all relevant UPPs, such as, for example, the obligation to ensure the security of personal information it holds.¹²⁴

8.72 Although non-government organisations contracted by NSW public sector agencies may come within the scope of the federal privacy regime, the Commission nonetheless believes that, as a matter of good administrative practice, an express requirement under the data security principle is necessary and desirable. This should, in the Commission's

122. ALRC DP 72 vol 2 Proposal 25-2; [25.88].

123. Cyberspace Law and Policy Centre, UNSW, *Best Practice Privacy Principles: Suggested Improvements to the ALRC's Model Unified Privacy Principles (UPPs)*, Submission to the Australian Government (2008), 23.

124. Cyberspace Law and Policy Centre, UNSW, *Best Practice Privacy Principles: Suggested Improvements to the ALRC's Model Unified Privacy Principles (UPPs)*, Submission to the Australian Government (2008), 23.

view, be reinforced by amending PPIPA as proposed in CP 3.¹²⁵ This will bring PPIPA in line with Commonwealth privacy law.

8.73 The Commission, consequently, does not recommend the adoption of UPP 8 in its current form. We propose that UPP 8 and PPIPA be amended as in the following recommendations.

RECOMMENDATION 10

UPP 8 should be amended as follows:

UPP 8. Data Security

8.1 An agency or organisation must take reasonable steps to:

- (a) ...
- (b) ...
- (c) *ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.*

RECOMMENDATION 11

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 a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an Information Privacy Principle if done or engaged in by the agency; and
- (2) to ensure that the contract does not authorise a contracted service provider for the contract to do or engage in such an act or practice.

THE COMMISSION'S CONCLUSIONS

8.74 In the interests of uniformity, the Commission generally supports the adoption of UPP 8 in respect of NSW agencies. In particular, we support:

- the terminology used in UPP 8, which reflects that already used in PPIPA and HRIPA;

125. See para 8.68.

- the criteria for data security contained in UPP 8.1(a), which also fundamentally reflect the criteria currently used in IPP 5(c) and HPP 5(1)(c); and
- the balance in UPP 8.1(b) between the often discordant data destruction and data retention requirements.

8.75 We acknowledge that, at a broad level, UPP 8 simplifies and consolidates current NSW data security obligations. However, the Commission does have two reservations about the formulation of UPP 8. First, the Commission queries whether UPP 8 will apply to require NSW agencies to ensure secure collection of information. For this reason, the Commission recommends PPIPA be amended to clarify that, unless otherwise stated, the privacy principles apply to personal information that is held, or collected for inclusion, in a record.

8.76 Second, the Commission urges the ALRC to reinstate the requirement to ensure the security of personal information that is disclosed to a third party contractor in an outsourcing arrangement. Although it may be redundant in relation to federal agencies, the same cannot be said for NSW agencies, where there is no statutory requirement on agencies to negotiate privacy clauses in contracts with service providers. Although the Commission recommends that such a provision be inserted into PPIPA, we believe it is desirable to include the requirement in the principle as well.

8.77 In the Commission's view, there is no need for a separate health privacy principle to apply to public sector health providers. Although there are differences in the way that health information should be managed in terms of the destruction and retention requirements of the data security principle, the Commission is satisfied that UPP 8 is able to accommodate those differences. The concept, under UPP 8, of retaining information for as long as it is needed for a lawful purpose under the UPPs is sufficiently broad to permit the prolonged retention of health information. The "authorised by law" exception also allows derogation from the obligations under the data security principle when other laws regulating health information expressly require or authorise an agency to engage in a contrary act or practice. Accordingly, the Commission does not consider it necessary to formulate a separate health privacy principle.

9. UPP 9: Access and correction

- Introduction
- NSWLRC Consultation Paper 3
- ALRC Discussion Paper 72
- ALRC Report 108
- Access
- Correction
- Refusal of request to access or correct
- Conclusion

INTRODUCTION

9.1 When an agency or organisation holds an individual’s personal information, legislation regulating the keeping of that information must also give the individual a right to access and, if necessary, correct it.

9.2 Privacy legislation is not the only legislation regulating the keeping of information, and hence rights to access and correct that information are given by Acts other than privacy Acts.¹ Rights of access and correction under these other Acts often interact, and sometimes clash, with privacy legislation. Key among such Acts is the freedom of information (“FOI”) legislation.²

9.3 The overlap between the access and correction provisions in the privacy legislation and those in other legislation creates complexity in both the Commonwealth and NSW, not only for agencies, but also for people seeking to access and correct personal information. As we pointed out in CP 3, the relevant provisions in both FOI and privacy Acts often regulate the same thing, but they do so in terms that are, at best, only similar or comparable to each other, not identical. At worst, it has been suggested that the differences between the Acts are such that it “is simply not possible” to obey them at the same time.³

9.4 The need to address this long standing confusion has been recognised in the past.⁴ In Report 108, the ALRC, although constrained by

-
1. This is only the case where information is held by public sector agencies.
 2. Key legislation includes the *Freedom of Information Act 1982* (Cth), the *Archives Act 1983* (Cth), the *Freedom of Information Act 1989* (NSW), the *Local Government Act 1993* (NSW) and the *State Records Act 1998* (NSW).
 3. NSW Law Reform Commission, *Privacy Legislation in New South Wales* Consultation Paper No 3 (2008) (“NSWLRC CP 3”) [8.5], also citing NSW Ombudsman, *Submission to the Review of the Privacy and Personal Information Act 1998*, 16, quoting former Privacy Commissioner, Chris Puplick.
 4. The FOI Act (Cth) predates the Privacy Act. It was intended that Part V of the FOI Act (Cth), which gives correction and annotation rights, would be transferred from the FOI Act into the privacy legislation “should the latter be enacted.” See Parliament of Australia, Senate Standing Committee on Legal and Constitutional Affairs, *Freedom of Information Act 1982 – The Operation and Administration of the Freedom of Information Legislation* (1987) [15.7] as cited by Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”), vol 1 [15.33]. This did not happen and hence the current situation, where both the Privacy Act and

the fact that it did not want to recommend amendments to the *Freedom of Information Act 1982* (Cth) (“FOI Act (Cth)”) given that it had a subsequent reference to review that Act,⁵ made some attempts to standardise access and correction procedures.

9.5 Since the publication of Report 108, however, several developments have taken place:

1. In July 2008, the federal government announced its intention to reform the FOI Act (Cth) in line with commitments made during the 2007 election. As a result, the Commonwealth Attorney-General asked the ALRC not to continue with its review of the Act. The ALRC had been due to report on its FOI reference by December 2008.⁶
2. Subsequently, in March 2009, the Commonwealth Cabinet Secretary and Special Minister of State announced the release of an exposure draft of the proposed Freedom of Information Amendment (Reform) Bill 2009 (Cth) and the Information Commissioner Bill 2009 (Cth). The “Companion Guide” to the exposure draft Bills indicated that the Government proposes to amend the *Privacy Act 1988* (Cth) “to enact an enforceable right of access to, and correction of, an individual’s own personal information, rather than maintain this right through the FOI Act”. This would “make the Privacy Act the key Commonwealth law for the collection, handling, disclosure and access to personal information”. The deadline for

the FOI Act give access and correction rights, came about. In their 1995 joint report the ALRC and the Administrative Review Council canvassed this issue, but decided not to recommend a change to the FOI Act (Cth). This conclusion was based in part on submissions the ALRC received indicating that many requests for information were “mixed”, in that they sought both personal and other information, and the system would become overly complex if such applications had to be dealt with in accordance with two different Acts: Australian Law Reform Commission and the Administrative Review Council, *Open Government: a review of the federal Freedom of Information Act 1982* (1995) [5.17].

5. See para 9.15-9.19.
6. Senator Faulker, Cabinet Secretary and Special Minister for State, (Media Release, 22 July 2008) «http://www.smos.gov.au/media/2008/mr_252008.html» at 9 June 2009.

submissions on this and accompanying Bills was 15 May 2009.⁷

3. On 6 May 2009, the Premier of NSW announced the release of a raft of public consultation drafts of Bills, including the Government Information (Public Access) Bill 2009 (NSW), the Government Information (Information Commissioner) Bill 2009 (NSW) and the Government Information (Public Access) (Consequential Amendments and Repeals) Bill 2009 (NSW). The deadline for submissions on these bills was 3 June 2009.⁸ The Bills passed through Parliament and the resulting Acts received Assent in June 2009. At the time of writing the three Acts were awaiting proclamation.
4. Simultaneously with the release of the draft bills, the government requested that the Commission “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* (NSW) or any successor legislation”. In undertaking this inquiry, the Commission is to have regard to “[t]he adequacy of the *Freedom of Information Act 1989* (NSW) (and any successor legislation) concerning the handling of access applications for personal information in ensuring effective protection of individuals' privacy”.⁹
5. Clause 1 of Schedule 1 of the *Government Information (Public Access) (Consequential Amendments and Repeals) Act 2009* (NSW) transfers Part 4 of the *Freedom of Information Act 1989*

7. Senator Faulker, Cabinet Secretary and Special Minister for State, *Freedom of Information (FOI) Reform Companion Guide* (March 2009), 14. The Guide says further that “[t]he co-location of privacy and FOI in a single office [which is the effect of the *Information Commissioner Bill 2009* (Cth)], and the future reform of the Privacy Act foreshadowed last year, is intended to strengthen and elevate the role and importance of privacy laws” (at 14).

8. NSW Department of Premier and Cabinet, FOI Reform – Open Government Information, «http://www.dpc.nsw.gov.au/prem/foi_reform__open_government_information» at 9 June 2009.

9. Terms of Reference received 1 June 2009, in addition to those received on 11 April 2006. See para 0.21

(NSW) (“FOI Act (NSW)”), which covers the amendment of records, to PPIPA. The Companion Guide to the Bills states that this has been done “pending the outcome of the Law Reform Commission’s review” of NSW privacy laws.¹⁰

9.6 As a consequence of all of the above, the landscape in relation to FOI legislation in general, and its interface with privacy legislation in particular, is currently evolving, not just at the Commonwealth level, but also in NSW. It is apparent from the foregoing (and from the discussion of UPP 9 below), that the Commonwealth is moving towards more access and correction provisions in relevant legislation. It can be inferred from the transfer of amendment provisions from the FOI legislation to PPIPA that the NSW Government is attempting to achieve the same. A further example of an attempt at rationalisation is that the *Government Information (Public Access) Act 2009* (NSW) contains a similar (although necessarily attenuated) definition of “personal information” to that used in PPIPA.¹¹

9.7 In the following discussion, we consider UPP 9, and compare it to current NSW law. At this stage, the Commission considers that UPP 9 is an adequate access and correction principle. However, because the law in NSW is subject to change, we cannot comment with finality on the matter of the inclusion of UPP 9 within the privacy principles that ought to apply in NSW. This chapter proceeds on this basis.

NSWLRC CONSULTATION PAPER 3

9.8 The Commission’s comments on access and correction principles in CP 3 highlighted the overlap problems in NSW. The Commission outlined the submission of Privacy NSW that the usefulness of s 14 and 15, which are the access and correction principles of PPIPA, is diminished by s 20(5) of PPIPA, due to a “lack of clarity about the breadth of [their] application”.¹² The Commission identified that the lack of clarity lay with

10. NSW Department of Premier and Cabinet, *Open Government Information – FOI Reform in New South Wales* (May 2009), 10.

11. *Government Information (Public Access) Act 2009* (NSW) sch 4, cl 4, *Privacy and Personal Information Protection Act 1998* (NSW) s 4.

12. NSWLRC CP 3 [6.32], citing Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998* (24 June 2004), 50. For the text of s 20(5) of the *Privacy and Personal Information Protection Act 1998* (NSW) see para 9.60.

s 20(5) of PPIPA (and its equivalent s 22(3) of HRIPA), rather than with s 14 and 15 themselves.¹³

9.9 The Commission went on to say that the difficulty with s 20(5) is the uncertainty, and lack of guidance, as to what are “conditions” or “limitations” of the FOI Act (NSW).¹⁴ We noted arguments made by Privacy NSW that it was uncertain exactly how “the access and correction provisions of the FOI Act relate to or are imported into” PPIPA. Privacy NSW cited as examples of this uncertainty questions as to whether s 20(5) had the effect of importing into PPIPA from the FOI Act (NSW): the requirement to lodge a request in writing, or to pay prescribed fees; the Schedule 1 list of exempt documents; the Schedule 2 list of exempt bodies; or the consultation requirements in Part 3. Privacy NSW concluded that the benefits of the less formal approach to request access to, or amendment of one’s own personal information in IPPs 7 and 8 are lost “if the request must in effect become an FOI application”.¹⁵

9.10 As a result of these comments, the Commission made the following proposal:

The meaning and effect of s 20(5) of the *Privacy and Personal Information Protection Act 1998* (NSW) and s 22(3) of the *Health Records and Information Privacy Act 2002* (NSW), and their application to the IPPs and HPPs respectively, should be clarified.¹⁶

9.11 The Commission also examined the relationship between s 13-15 of PPIPA and Parts 2-4 of the FOI Act (NSW). We noted that it is because the relevant provisions of the two Acts are similar, rather than identical, that the duplications produce inconsistencies.¹⁷ The Commission raised the two following issues:

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

13. NSWLRC CP 3.

14. NSWLRC CP 3 [6.33], citing Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998* (24 June 2004), 82.

15. NSWLRC CP 3 [6.34], citing Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998* (24 June 2004), 83.

16. NSWLRC CP 3 Proposal 13.

17. NSWLRC CP 3 [8.9].

- Should the *Freedom of Information Act 1989* (NSW) be the means by which the *Privacy and Personal Information Protection Act 1998* (NSW) access rights are obtained?¹⁸

9.12 We received submissions addressing both the issues and the proposal above. Most submissions agreed with proposal 13, that the meaning and effect of s 20(5) of PPIPA and 22(3) of HRIPA should be clarified. The Australian Privacy Foundation, for example, agreed that the meaning of s 20(5), and the relationship between PPIPA and the FOI Act (NSW), should be clarified and submitted that “[i]f anything, first party access requests should be exclusively covered by PPIPA, not the FOI Act”.¹⁹ In response to the issues, the Public Interest Advocacy Centre (PIAC) also submitted “that the right to access and correct one’s personal information should be dealt with under the PPIP Act and the corresponding provisions of the *Freedom of Information Act 1989* (NSW) and the *Local Government Act 1993* (NSW) should be repealed”.²⁰ PIAC also submitted that “[s]ection 5 and subsection 20(5) of the PPIP Act should be repealed”.²¹ The Legal Aid Commission of NSW likewise did not “support the proposal to remove access and correction principles from the privacy legislation”.²² The Legal Aid Commission suggested that “[r]ather than resolving these problems of overlap by removing access and correction rights under privacy, we consider that both legislative schemes could be improved to complement rather than contradict each other”.²³ Privacy NSW submitted that it supported “the continued inclusion of the access and amendment provisions for personal information within the Privacy and Personal Information Protection Act”.²⁴

9.13 However, a number of submissions supported the suggestion that the FOI Act (NSW) be the sole vehicle for the access and correction of personal information. The Department of Community Services indicated that it “strongly support[ed] the Ombudsman’s recommendation that the FOI Act be the means by which the PPIPA access and correction rights are

18. NSWLRC CP 3 Issues 62 and 63.

19. Australian Privacy Foundation, *Submission*, 9 and 15.

20. Public Interest Advocacy Centre, *Submission*, 32.

21. Public Interest Advocacy Centre, *Submission*, 33.

22. Legal Aid Commission of NSW, *Submission*, 6.

23. Legal Aid Commission of NSW, *Submission*, 7.

24. Privacy NSW, *Submission*, 1.

obtained”.²⁵ The Department of Corrective Services also supported the proposal in issue 63, noting that it already encouraged those making applications to access or correct their personal information to do so in accordance with the FOI Act (NSW).²⁶ The State Records and the Law Society of NSW also supported the concentration of these provisions in the FOI Act (NSW).²⁷

9.14 The Commission will consider these submissions in its remaining review of privacy law and of access to personal information.

ALRC DISCUSSION PAPER 72

9.15 In DP 72, the ALRC noted that it had “considered various models for dealing with the overlap”.²⁸ It ultimately proposed that a new part covering access and correction of personal information held by agencies be inserted into the Privacy Act.²⁹ The ALRC further proposed that Part V of the FOI Act (Cth) be repealed, and a section inserted in its stead providing that access to and correction of personal information be dealt with under the Privacy Act.³⁰ In reaching these proposals, it concluded that the problem of “mixed” applications could be solved administratively by agencies.³¹ The ALRC felt that the abilities both to access and correct personal information were “fundamental privacy rights” and, as such, belonged in privacy legislation overseen by the Privacy Commissioner.³²

9.16 The model access and correction UPP initially formulated by the ALRC therefore only applied to personal information held by organisations, with the new part applying to agencies.³³ In this, it was singular among the UPPs, which, as explained in the Introduction, and as

25. NSW Department of Community Services, *Submission*, 5.

26. NSW Department of Corrective Services, *Submission*, 6-7.

27. NSW State Records Office, *Submission*, 2, Law Society of NSW, *Submission*, 16.

28. Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No 72 (2007) (“ALRC DP 72”) vol 1 [12.37].

29. ALRC DP 72 Proposal 12-6.

30. ALRC DP 72 Proposal 12-7.

31. ALRC DP 72 vol 1 [12.41].

32. ALRC DP 72 vol 1 [12.39].

33. ALRC DP 72 Proposal 26-1.

their name implies, were designed to provide a uniform framework for the handling of personal information.

ALRC REPORT 108

9.17 Two factors caused the ALRC to modify its DP 72 position in the final report. First, following the release of DP 72, the then Attorney-General, The Hon. Philip Ruddock, asked the ALRC to review the FOI Act (Cth). The ALRC decided that proposed changes to the FOI Act (Cth) should be left to that future review.³⁴ Secondly, submissions received by the ALRC in response to DP 72 objected to the proposal to keep the obligations for agencies separate from those for organisations, and also indicated that this approach would not address any of the issues arising from the overlap of privacy and FOI legislation.³⁵

9.18 In Report 108, therefore, the ALRC moved away from its DP 72 proposals. The ALRC expressed the view that the access and correction principle, UPP 9, should instead provide a “predominately unified” regime for access and correction.³⁶ The ALRC accepted the submissions it received on this point and noted that a “single regime” for the access and correction of documents, whether held by agencies or organisations, was the preferred approach.³⁷ Although amendments to the FOI Act (Cth) were not considered appropriate at this stage, the ALRC concluded that

34. ALRC Report 108 vol 1 [15.48]-[15.51]. Work was stopped on the FOI reference following further developments; see para 9.5.

35. In relation to the submissions it received regarding this proposal, the ALRC stated that, while some supported it, others submitted that the access and correction principle should apply to agencies as well. There were a number of reasons behind this failure to support the proposal, including that having separate provisions for agencies and organisations “would create confusion; contradict the aim of creating a single set of privacy principles; and would not address the problems caused by requests for access to documents containing both personal and non-personal information, or a mix of information about two or more individuals”. The ALRC also pointed out that other submissions did not support the repeal of Part V of the FOI Act (Cth). The reasons given included that “the FOI Act is already adequately structured to accommodate the access and correction provisions”. The ALRC also noted that the “OPC submitted that it would be more appropriate to expand the correction rights under the FOI Act to be consistent with those in the *Privacy Act*”. See ALRC Report 108 vol 1 [15.39]-[15.41] and accompanying footnotes.

36. ALRC Report 108 vol 2 [29.3].

37. ALRC Report 108 vol 1 [15.50].

the problems caused by the overlap could be lessened in the interim by maintaining “the existing arrangements whereby individuals have rights of access to and correction of, personal information under both the Privacy Act and the FOI Act” but modifying “the provisions that deal with the interaction between the access and correction provisions under both Acts”.³⁸

9.19 Recommendation 29-1 of Report 108 therefore states that the UPPs should “contain a principle called ‘Access and Correction’ that, subject to Recommendation 29-2, applies consistently to agencies and organisations”.³⁹ Recommendation 29-2 states that, where personal information is held by an agency, any exemptions to the general rule that access must be provided should be those found in relevant Commonwealth law but, where it is held by an organisation, the applicable exemptions should be those that currently appear in NPP 6.⁴⁰

9.20 As is examined in more detail below, UPP 9 provides that the exemptions contained within the FOI Act (Cth) relating to when agencies do not have to provide access to documents in their possession still apply to personal information.⁴¹ A separate set of exemptions, applicable only to organisations, is then set out within the UPP itself. However, the ALRC has recommended that the FOI provisions relating to procedure for access and correction (or amendment as it is known under the FOI Act (Cth)),⁴² and also the limitations placed on the amendment of personal information by Part V of the FOI Act (Cth), should no longer apply to requests for correction of personal information made under the Privacy Act. Yet it will remain possible to make an application for access or correction of personal information under the FOI Act (Cth) and the provisions of that Act will, of course, still apply to such applications.

9.21 As a result, UPP 9 does not, and indeed cannot, entirely address the problems arising from the overlap between the Privacy Act and the

38. ALRC Report 108 vol 1 [15.47]-[15.48].

39. ALRC Report 108 vol 2 Recommendation 29-1.

40. ALRC Report 108 vol 2 Recommendation 29-1(a) and (b).

41. See ALRC Report 108 vol 2 Recommendation 29-2.

42. The *Freedom of Information Act 1982* (Cth) and the *Freedom of Information Act 1989* (NSW) both refer to the “amendment” of documents, as does the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) but, for convenience, this chapter mostly refers simply to “correction” of information.

FOI Act (Cth). Further work will need to be done in this area at the Commonwealth level in order to achieve a clear and consistent regime for the access and correction of personal information.

9.22 In Report 108, the ALRC speculated that the then anticipated review of the FOI Act “could consider amending the FOI Act so that it no longer regulates access to, and correction of, personal information and is limited to regulating access to information about third parties and deliberative processes of government”.⁴³ Other options that such a review might consider could be the amendment of the FOI Act (Cth) “to provide a simpler and more user-friendly process” for the access and correction of personal information, the amendment of the exemptions to access under the FOI Act (Cth) and the “expansion of the correction rights under the FOI Act to accord with those under the Privacy Act”.⁴⁴ These are all options that the NSWLRC might explore in our future consideration of these issues.

9.23 A further consequence of UPP 9 in its current form is that, if the States and the Commonwealth continue to have different FOI regimes, then, even if they adopt UPP 9, its effect will be different in practice. In Report 108, the ALRC noted a submission to DP 72 in relation to the proposal to amend the FOI Act (Cth) and the Privacy Act which the ALRC summarised as follows:

National Legal Aid submitted that the proposal has implications in relation to the national consistency of privacy laws relating to the federal and state public sectors. It noted that some state privacy laws are subordinated to freedom of information laws and access to personal information is subject to FOI exemptions.⁴⁵

9.24 The fact that the ALRC has formulated a UPP covering agencies and organisations does not make this less applicable. In NSW, for instance, legislative change beyond the mere adoption of the UPP would be required in order to achieve consistency. For this reason, further work will need to be done if true uniformity is to be achieved.

43. ALRC Report 108 vol 1 [15.51].

44. ALRC Report 108 vol 1 [15.52].

45. ALRC Report 108 vol 1 [15.42].

ACCESS

UPP 9

9.25 UPP 9 provides as follows in respect of access:

- 9.1 If an agency or organisation holds personal information about an individual and the individual requests access to the information, it must respond within a reasonable time and provide the individual with access to the information, except to the extent that:

Where the information is held by an agency:

- (a) the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; or

Where the information is held by an organisation:

- (b) providing access would be reasonably likely to pose a serious threat to the life or health of any individual;
- (c) providing access would have an unreasonable impact upon the privacy of individuals other than the individual requesting access;
- (d) the request for access is frivolous or vexatious;
- (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings;
- (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- (g) providing access would be unlawful;
- (h) denying access is required or authorised by or under law;
- (i) providing access would be likely to prejudice an investigation of possible unlawful activity;
- (j) providing access would be likely to prejudice the:
- (i) 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) enforcement of laws relating to the confiscation of the proceeds of crime;
- (iii) protection of the public revenue;
- (iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
- (v) preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

- (k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

9.2 Where providing access would reveal evaluative information generated within the agency or organisation in connection with a commercially sensitive decision-making process, the agency or organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: The mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information under UPP 9.2.

9.3 If an agency or organisation is not required to provide an individual with access to his or her personal information it must take such steps, if any, as are reasonable to provide the individual with as much of the information as possible, including through the use of a mutually agreed intermediary.

9.4 If an organisation charges for providing access to personal information, those charges:

- (a) must not be excessive; and
- (b) must not apply to lodging a request for access.

Note: Agencies are not permitted to charge for providing access to personal information under UPP 9.4.

- 9.5 An agency or organisation must provide personal information in the manner requested by an individual, where reasonable and practicable.

Current Commonwealth law

Personal information held by agencies

9.26 Under the Privacy Act, Principle 6 regulates access to personal information in the possession of Commonwealth agencies. It states:

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 6 is silent as to how applications for access are to be dealt with.

Personal information held by organisations

9.27 Where personal information is held by organisations, the relevant privacy principle is NPP 6, which simply provides that:

If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual.

9.28 Unlike Principle 6, NPP 6 goes on to list the circumstances in which the organisation does not have to provide access.⁴⁶ Under Principle 6, a record-keeper must have reference to “the applicable provisions of any law of the Commonwealth” in order to determine whether or not they are authorised to refuse access.

How and why is UPP 9 different from current Commonwealth law relating to the access of personal information?

9.29 In relation to access, UPP 9 is, for the most part, simply a hybrid of Principle 6 and NPP 6. While it does depart from the current access principles in a number of ways, these changes are not significant. The following paragraphs describe the changes and the rationale behind them.

46. See NPP 6.1(a)-(k).

General access principle

9.30 NPP 6 is expressed in terms of an obligation on an organisation to provide access and Principle 6 is expressed in terms of a right for individuals to gain such access. The ALRC proposed in DP 72 that the UPP should adopt the language of NPP 6, in preference to Principle 6, and “be expressed as an obligation”.⁴⁷ It did not receive any submissions in opposition to this proposal. UPP 9.1 has therefore been drafted to bestow an obligation on an agency or organisation to provide access, rather than grant an individual the ability to gain it. This form is consistent with that of the other model UPPs.⁴⁸

9.31 The ALRC also recommended that UPP 9, similarly to NPP 6, apply to information that an agency or organisation “holds” rather than information in its “possession or control”, (in contrast to Principles 6 and 7). The ALRC was of the view that the word “holds” should be capable of an interpretation that incorporates “constructive possession” of documents, so that, where personal information “is in the control of one agency or organisation and the possession of another”, individuals are able to issue their request to the agency that actually possesses the information.⁴⁹ The ALRC stated that, if Parliamentary Counsel does not agree with the view that “holds” can be read in such a way, then the UPP should be drafted in another manner that does extend to constructive possession.⁵⁰

Exemptions for agencies

9.32 One of the questions raised by the ALRC in DP 72 was whether the exemptions applicable to agencies under the Privacy Act should be the same as those to which they were subject under the FOI Act (Cth). Some submissions said that the exemptions should remain the same, while others suggested that they be changed.⁵¹ In Report 108, the ALRC concluded that the exemptions covering agencies in UPP 9 should be the same as the exemptions in the FOI Act (Cth) and other relevant Commonwealth law, such as the *Archives Act 1983* (Cth).

47. ALRC DP 72 vol 1 [12.43], Proposal 12-8(a).

48. ALRC Report 108 vol 2 [29.25]-[29.26].

49. ALRC Report 108 vol 2 [29.29].

50. ALRC Report 108 vol 2 [29.31].

51. ALRC Report 108 vol 2 [29.41]-[29.43].

9.33 The rationale given for this conclusion was that agencies should not be expected to comply with two sets of possibly conflicting exemptions relating to the same information, nor should individuals be able to access information under the Privacy Act that would not be available under the FOI Act (Cth).⁵² As discussed in the introduction above, the ALRC considered that the question of whether any revision of the exemptions in the FOI Act (Cth) was required in order to deal with requests for personal information was one for the then anticipated review of that Act rather than Report 108.⁵³ As a result, the exemptions that appear in UPP 9 apply only to organisations.

9.34 On the face of it, there does not seem to be a reason why exemptions to the need to provide access to personal information should not be standardised. This is an issue that we shall explore in our review of FOI and access to personal information.

Exemptions for organisations

9.35 The exemptions applicable to organisations are the same as those contained in NPP 6, apart from one change. This relates to information that may be a threat to a person's life or health, which is discussed below. There is also a change to the Note to NPP 6.2 but this is to clarify the effect of NPP 6.2 rather than change the sub-principle in any way. The Note to NPP 6.2 states:

An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

9.36 The ALRC agreed with the Cyberspace Law and Policy Centre that the Note is tautologous and should be removed.⁵⁴ The ALRC has recommended that the following Note be substituted:

The mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information under UPP 9.2.

52. ALRC Report 108 vol 2 [29.44].

53. ALRC Report 108 vol 2 [29.44]-[29.47].

54. ALRC Report 108 vol 2 [29.58], [29.64].

This allays concerns expressed in some submissions that UPP 9.2 might be used as a way of refusing direct access in circumstances where it should be provided.

9.37 Otherwise, the ALRC concluded that UPP 9 should include the existing exemptions in NPP 6 because, in its view, these had achieved the appropriate balance between “the public interest in safeguarding the handling of personal information” and other “competing public interests”.⁵⁵

Threat to life or health

9.38 NPP 6.1(a) provides that access does not have to be granted to an individual where the provision of information, other than health information, “would pose a serious *and imminent* threat to the life or health of any individual”. NPP 6.1(b) provides that access to health information does not have to be granted where it “would pose a serious threat to the life or health of any individual”. In accordance with Proposal 26-6 of DP 72, the ALRC has merged NPP 6.1(a) and (b) into one provision, UPP 9.1(b), eliminating the requirement that the threat be “imminent”.⁵⁶ The reason behind this proposal was that it was “too difficult to establish” that a threat “to the life or health of any individual” was “serious and imminent”. According to the ALRC, as long as the exception could be applied when the threat was serious, an organisation might be able to take steps to stop it becoming imminent.⁵⁷

9.39 The submissions received by the ALRC that commented upon this proposal were mostly in support of it.⁵⁸ The Office of the Federal Privacy Commissioner, (“OPC”) however, argued that the test of imminence should be maintained for information other than health information.⁵⁹ The OPC was concerned that the removal of this requirement would lead to a reduction in the level of privacy protection. It suggested that any difficulties that arose in the application of the “serious and imminent”

55. ALRC Report 108 vol 2 [29.63].

56. ALRC DP 72 Proposal 26-6, also see vol 2 [26.58].

57. ALRC DP 72 vol 2 [26.57].

58. ALRC Report 108 vol 2 [29.53].

59. Office of the Federal Privacy Commissioner, *Submission PR 499*, cited by ALRC Report 108 vol 2 [29.54].

test could be met by “guidance issued by the [OPC] and increased education of decision makers”.⁶⁰

9.40 The ALRC noted that an increased likelihood that an individual might be refused access to personal information on the ground that the information poses “a serious threat to the life or health of any individual” could result from the removal of the imminence requirement. However, the ALRC also noted that it had made further recommendations that will lessen the disadvantage caused by the removal of the requirement, including a more rigorous intermediaries provision.⁶¹ This recommendation is reflected by UPP 9.3, which is discussed below.⁶²

Commercially sensitive information

9.41 UPP 9.2 extends the applications of NPP 6.2 to agencies so that they do not have to reveal evaluative information produced within the agency in connection with a commercially sensitive decision-making process. Where an agency does not function to generate a profit, applying UPP 9.2 could prove problematic.⁶³ In those circumstances, some direction may need to be given as to the meaning of “commercially sensitive”, for example, in order to ensure that this principle corresponds with the exemptions in the FOI legislation to which agencies are subject.

Intermediaries

9.42 NPP 6.3 states that, if an organisation is not required to provide a person with the information they have requested as a result of one of the exemptions contained within NPP 6.1, it must, “if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties”.

60. Office of the Federal Privacy Commissioner, *Submission PR 499*, 20 December 2007. The decision not to include the requirement that a threat be “imminent” as well as “serious” in UPP 9 is consistent with the ALRC’s proposed use and disclosure UPP, UPP 5, and reflects the reasoning given in relation to that UPP: ALRC Report 108 vol 2 [29.59]. See also para 5.27-5.30 for a discussion of the use and disclosure principle, including on the rationale for the removal of the “imminent” requirement in that instance.

61. ALRC Report 108 vol 2 [29.62].

62. See para 9.42-9.47.

63. State-owned corporations are one exception.

9.43 UPP 9.3 is modelled on NPP 6.3. While formerly only applicable to organisations, it has been extended to cover agencies too. However, agencies are currently subject to s 41(3) of the FOI Act (Cth), which provides that, where information is requested and “disclosure of the information might be detrimental to the applicant’s physical or mental health or well-being” the information can be given to a “qualified person” instead of to the applicant.⁶⁴ The exposure draft Freedom of Information Amendment (Reform) Bill 2009 would repeal this section of the FOI Act (Cth).⁶⁵ The provision that replaces it, however, still refers to a “qualified person”.⁶⁶ It is possible that either UPP 9.3 will need to be amended so it reflects the FOI Act (Cth), or this matter will need to be addressed in the Privacy Commissioner’s Guidelines.

9.44 In DP 72, the ALRC proposed that the model ‘Access and Correction’ UPP should provide that, in circumstances where an exception to the general rule applies:

the organisation must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, that would allow for sufficient access to meet the needs of both parties.⁶⁷

9.45 The text of the UPP recommended in Report 108 varies slightly from that proposed in DP 72. The ALRC has included the words “if any” following the words “such steps” in order to make it clear that agencies and organisations should not be compelled to take any steps in circumstances where none would be reasonable or available.⁶⁸ The words “to reach an appropriate compromise” that appeared in the DP 72 formulation have been removed due to the potential ambiguity of those words.⁶⁹ The requirement that the compromise “allow sufficient access to meet the needs of both parties” has also been taken out because the ALRC

64. *Freedom of Information Act 1982* (Cth) s 41(3). A “qualified person” is defined in s 41(8) as a person occupied in “the provision of care for their well-being, and, without limiting the generality of the foregoing, includes any of the following: (a) a medical practitioner; (b) a psychiatrist; (c) a psychologist”.

65. Freedom of Information Amendment (Reform) Bill 2009 (Cth) s 24.

66. Freedom of Information Amendment (Reform) Bill 2009 (Cth) s 47 F.

67. ALRC DP 72 Proposal 26-2.

68. ALRC Report 108 vol 2 [29.76]. This change was made following submissions from the Australian Federal Police and the Australian Communications and Media Authority.

69. ALRC Report 108 vol 2 [29.78].

agreed with submissions it received that suggested this requirement might limit the operation of the principle. The ALRC noted, for example, that there might be situations in which the compromise reached does not accommodate the needs of both parties but is still preferable to a blanket refusal to allow access.⁷⁰ The ALRC has also rearranged the model principle so that it is clear that the use of an intermediary is not the only way in which a compromise as to the access of information can be reached.⁷¹

9.46 The ALRC further noted that the model UPP as currently drafted is limited to situations where the parties can agree on an intermediary and does not set out a process for circumstances in which no intermediary can be mutually agreed. The ALRC took the view that the process it recommended in relation to health information would cover a sufficient number of situations that arose under UPP 9.3, as a large proportion of access complaints relate to health information. It recommended that:

where an organisation denies an individual access to his or her health information on the grounds that it is reasonably likely to pose a serious threat to any individual, the individual should have the right to nominate a health service provider and request that the organisation provide the nominated health service provider with access to the information.⁷²

9.47 In addition, the ALRC pointed out that it might be possible for the Privacy Commissioner to act as an intermediary in some situations.⁷³

Procedural Requirements

9.48 The ALRC has recommended that the procedural sections of UPP 9 (UPP 9.4 and 9.5) regulate not only organisations, but also agencies. This represents a shift away from the current position, in which the procedures used by agencies to enable people to access personal information primarily seem to be those set out in the FOI Act (Cth).⁷⁴

70. ALRC Report 108 vol 2 [29.79].

71. ALRC Report 108 vol 2 [29.82].

72. ALRC Report 108 vol 2 [29.80].

73. ALRC Report 108 vol 2 [29.81].

74. The Federal Privacy Commissioner's Information Privacy Principles Guidelines advise agencies in receipt of requests for access to personal information to handle them "under its normal access processes, which will include, but may not be restricted to FOI". The Guidelines further state that the Privacy

9.49 As discussed previously, in DP 72 the ALRC proposed that a new part dealing with access and correction to personal information held by agencies be included in the Privacy Act.⁷⁵ The ALRC further proposed that the new part should contain provisions detailing the procedures to be followed by agencies in the receipt of a request for access to personal information.⁷⁶ It stated that the procedures to be included in the new part should be “similar to, but less onerous than” those in the FOI Act (Cth).⁷⁷

9.50 The ALRC received a number of submissions supporting this proposal.⁷⁸ The OPC, however, submitted that it was not “convinced that all procedural matters needed to be set out in legislation, as opposed to being subject to guidance” issued by the Office.⁷⁹ The OPC suggested that any procedural requirements for agencies dealing with access requests that were included in the Privacy Act should be as similar as possible to the proposed UPP (which at that stage was only proposed to apply to organisations).⁸⁰

9.51 In Report 108, the ALRC stated that “an individual seeking access to personal information should not be subject to the FOI Act process

Commissioner did not set up separate administrative systems for Principle 6, since the FOI Act (Cth) already provided a procedural framework for the access of information, including personal information (see Office of the Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4-7* (1988) «http://www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_15.7.pdf» 13, at 26 March 2009). The Centrelink website, for example, sets out the process for the access of personal information as one that is FOI in character (see Centrelink, Freedom of Information (FOI) «<http://www.centrelink.gov.au/internet/internet.nsf/legal/foi.htm>» (undated) at 26 March 2009). The form required for access or correction of personal information, which is accessible via the site, is headed “Freedom of Information: I want to access or change document(s)” (see Centrelink, “Freedom of Information: I want to access or change documents” Form Si031 «[http://www.centrelink.gov.au/internet/internet.nsf/filestores/si031_0808/\\$file/si031_0808en_p.pdf](http://www.centrelink.gov.au/internet/internet.nsf/filestores/si031_0808/$file/si031_0808en_p.pdf)» (undated) at 26 March 2009).

75. ALRC DP 72 Proposal 12-6. See para 9.15.

76. ALRC DP 72 Proposal 12-11.

77. ALRC DP 72 vol 1 [12.59].

78. ALRC Report 108 vol 2 [29.143].

79. Office of the Federal Privacy Commissioner, *Submission PR499*, as cited by ALRC Report 108 vol 2 [29.144].

80. Office of the Federal Privacy Commissioner, *Submission PR499*, as cited by ALRC Report 108 vol 2 [29.144].

where a simpler process can be established”. Accordingly, the ALRC found that it was “appropriate” for agencies to be subject to the same procedures as organisations, in relation to applications for access to personal information.⁸¹ For reasons discussed above, the ALRC had by now moved away from its DP 72 proposal to amend both the Privacy Act and the FOI Act (Cth).⁸²

9.52 The ALRC progressed from the statement that agencies and organisations should be regulated by the same procedural principles into a discussion of what the content of these principles should be. It did not canvass issues such as how the long standing use of the more prescriptive FOI procedure would change, or whether the Privacy Act or FOI Act (Cth) should be amended to state explicitly that the provisions of the latter pertaining to procedures for access are no longer relevant to personal information (although it does recommend that the OPC “develop guidance for agencies and organisations” about access and correction, including the need to reduce barriers to access of personal information).⁸³ If the UPP 9 is to be effective, these are issues that will need to be resolved at some point. Otherwise, the underlying confusion regarding the overlap between the Acts will remain. Given that we do not at this stage know what shape the Commonwealth FOI legislation will take it is not possible to comment further on this point.

Fees

9.53 UPP 9.4 relates to the fees that may be charged for access to personal information and is, apart from the addition of a Note, the same as NPP 6.4. NPP 6.4 states that, if an organisation charges fees for the provision of access to personal information, those fees “must not be excessive” and “must not apply to lodging a request for access”. Agencies are currently not able to charge for the provision of access to personal information.⁸⁴ The ALRC has recommended the inclusion of the following Note to 9.4 to clarify that organisations may continue to charge a fee for provision of access to personal information, but agencies may not:

Agencies are not to charge for providing access to personal information under UPP 9.4.

81. ALRC Report 108 vol 2 [29.146].

82. See para 9.17-9.19.

83. ALRC Report 108 vol 2 [29.167].

84. ALRC Report 108 vol 2 [29.160].

9.54 The ALRC noted that it had “not been made aware of any issues” associated with the inability of agencies to render charges for access to personal information. It expressed the view that “individuals should not be disadvantaged by seeking to assert their privacy interests”, and one way of preventing disadvantage from occurring was to minimise any costs involved.⁸⁵ Due to the existence of a “public interest in an individual being able to access and correct information that an agency holds about him, or her”, the ALRC considered that an agency should remain liable for any related costs.⁸⁶

Timeliness

9.55 The ALRC recommended that the access and correction UPP should “contain a requirement that agencies and organisations must respond to requests for access to personal information within a reasonable time”.⁸⁷ Since responding to requests for access made under NPP 6 in a timely way was already considered “best practice”⁸⁸, and the proposed requirement “generally would not impose higher obligations on an agency” than those contained within the FOI Act (Cth), the ALRC noted that it did not anticipate that the inclusion of this requirement would create a further administrative burden for either organisations or agencies.⁸⁹ UPP 9.1 therefore provides that, where an agency or organisation receives a request for access to personal information, “it must respond within a reasonable time”.

Manner of providing access

9.56 UPP 9.5 creates a requirement that did not formerly exist explicitly in the NPP, which is that “agencies and organisations must provide information in the manner requested by an individual, where reasonable and practical”.⁹⁰ The ALRC stated that it was “arguable”, although not “self-evident”, that such a requirement could already be implied in NPP 6. The express inclusion of the provision is designed to “promote clarity in the access and correction requirements”. The ALRC further said that such a requirement is consistent with those already present for

85. ALRC Report 108 vol 2 [29.160].

86. ALRC Report 108 vol 2 [29.161].

87. ALRC Report 108 vol 2 [29.162].

88. ALRC Report 108 vol 2 [29.162], citing J Douglas-Stewart, *Annotated Privacy Principles* (2005) [7.3740].

89. ALRC Report 108 vol 2 [29.162].

90. ALRC Report 108 vol 2 [29.163], UPP 9.5.

agencies in the FOI Act (Cth).⁹¹ Section 20 of the FOI Act (Cth) sets out a series of “forms of access” via which access to a document may be given to an applicant. It then provides that:

Subject to subsection (3) and to section 22, where the applicant has requested access in a particular form, access shall be given in that form.⁹²

9.57 Subsection (3) contains a number of circumstances in which access does not have to be given in the requested form, while s 22 allows for the deletion of exempt material from documents.⁹³ It is questionable whether this provision is narrower than UPP 9.5, and also whether UPP 9.5 increases the burden on agencies to provide access in the manner requested in a way that is reasonable.

Current law in NSW

9.58 IPP 6 (PPIPA s 13) provides that agencies holding information about a person “must take such steps as are, in the circumstances, reasonable” to enable that person to determine if the agency in question holds information about them, and, if so, what the purposes are for the retention of that information, and what their entitlement to gain access to it is.⁹⁴ IPP 7 (PPIPA s 14) directs agencies upon request to provide an individual access to personal information held regarding him or her “without excessive delay or expense”.⁹⁵

9.59 HPPs 6 and 7, which appear in HRIPA and regulate access to health information, are drafted in nearly the exact terms as IPPs 6 and 7.⁹⁶ In addition, Division 3 of HRIPA sets out the procedure for access to health information held by private sector providers. Section 29, in Division 3, sets out the “situations where access need not be granted”.

9.60 As is the case at the Commonwealth level, these principles are not the only provisions governing access to personal and health information held by NSW agencies. Section 5 of PPIPA states that nothing in that Act

91. ALRC Report 108 vol 2 [29.163].

92. *Freedom of Information Act 1982* (Cth) s 20(2).

93. *Freedom of Information Act 1982* (Cth) s 20(3), 22.

94. *Privacy and Personal Information Protection Act 1998* (NSW) s 13.

95. *Privacy and Personal Information Protection Act 1998* (NSW) s 14.

96. *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 6-8.

is to affect the operation of the FOI Act (NSW). In addition, as discussed above, s 20(5) of PPIPA provides:

Without limiting the generality of section 5, the provisions of the *Freedom of Information Act 1989* that impose conditions or limitations (however expressed) with respect to any matter referred to in sections 13, 14 or 15 are not affected by this Act, and those provisions continue to apply in relation to any such matter as if those provisions are part of this Act.⁹⁷

9.61 Section 22(3) of HRIPA is equivalent to s 20(5). HPP 7 also contains a statutory note advising that access to information held by public sector health care providers is also available under the FOI Act (NSW).⁹⁸ As a result of these provisions, access to personal and health information held by public sector agencies under either PPIPA or HRIPA is subject to any relevant provisions of the FOI Act (NSW).

9.62 In order to find exemptions to IPP 7, it is necessary to look to the FOI Act (NSW).⁹⁹ The circumstances in which access to information may be refused under the FOI Act (NSW) are set out in s 25 of that Act. They include where the document is an exempt document. The kinds of documents that are exempt from access are then listed in Schedule 1.¹⁰⁰

9.63 Clause 6 of Schedule 1 provides that documents containing information that might lead to the disclosure of “the personal affairs of any person” may be exempt if the applicant is not the person that the information relates to. Under s 31 of the FOI Act (NSW), an agency cannot give access to a document containing personal information about a person other than the applicant without first taking reasonable steps to consult the person whom the information is about in order to determine whether or not the document is exempt under Clause 6. In addition, s 31(4) provides that, in circumstances where an applicant seeks documents containing personal information that is considered to be potentially detrimental to their “physical or mental health”, it is sufficient

97. *Privacy and Personal Information Protection Act 1998* (NSW) s 20(5), see also para 9.8-9.10.

98. *Health Records and Information Privacy Act 2002* (NSW) sch 1, cl 7.

99. *Freedom of Information Act 1989* (NSW) s 25 and sch 1.

100. Apart from the obvious exemptions of cabinet and executive council documents, other exemptions include, but are not limited to, documents subject to legal professional privilege, those relating to the internal workings of agencies and those relating to business affairs.

if the documents are “given to a registered medical practitioner nominated by the applicant”.

9.64 The interaction between s 14, 15 and s 20(5) of PPIPA and the FOI Act (NSW) is not altogether clear, as is discussed below.

How does NSW law differ from UPP 9?

9.65 The comparative exercise engaged in here is complicated both by the lack of clarity in the present NSW law,¹⁰¹ as well as by the fact that the ground is shifting as we write.¹⁰² This is particularly so insofar as the provisions under consideration deal with procedural matters.

9.66 An example of the difficulties the Commission presently faces arises in relation to the issue of fees. UPP 9, as discussed above, states that fees cannot be charged for allowing access to personal information. IPP 7 provides that, where a request is made for personal information, that information should be provided “without excessive delay or expense”. According to Privacy NSW, this means that agencies cannot charge for access to personal information where an application is made under PPIPA. If an application is made under the FOI Act (NSW), the agency is currently able to charge fees. Agencies are also allowed to charge fees for the access of documents if the Acts that they administer allow them to do so.¹⁰³ This illustrates that what happens in practice is not always clear from the principles themselves. Further obscuring the issue is the fact that the public consultation draft of the *Government Information (Public Access) Act 2009* provides that, in relation to applications for access to personal information, agencies “cannot impose any processing charge for the first 20 hours of processing time for the application”.¹⁰⁴

9.67 As discussed in the introduction to this chapter, the Commission has been asked to review the access provisions of the new FOI legislation. The comparison between NSW law and the UPP is best left for a subsequent report. The comparisons below are therefore merely preliminary.

101. See para 9.3, 9.8-9.10.

102. See para 9.5-9.6.

103. Privacy NSW, *Consultation*.

104. *Government Information (Public Access) Act 2009* (NSW) s 67.

Information covered by the IPPs

9.68 Since IPPs 6 and 7, and UPP 9, each import other relevant legislation, in particular FOI legislation, the above statement is particularly true in relation to any attempt to compare them. As mentioned earlier, the Commission may decide to recommend in its future report that the exemptions to access to personal information be the same for both agencies and organisations.

Information covered by the HPPs

9.69 HPP 7(2) provides that an organisation does not have to grant access under HPP 7(1) if it is “lawfully authorised or required not to comply with the provision”, or “non-compliance is otherwise permitted” by an Act or other law.¹⁰⁵ Section 29 of HRIPA lists the situations in which access to information does not have to be granted by private sector health care providers. These situations are similar to those listed in UPP 9.1, although there are some differences.

9.70 Section 29(a), like UPP 9.1(b), deals with circumstances in which the release of information “would pose a serious threat” to the health of any individual. It does not contain the extra requirement currently present in NPP 6.1(b) that the threat must not only be serious but also “imminent”.¹⁰⁶ However, s 29(a) contains the additional proviso that a refusal made in accordance with it must also accord with any relevant privacy guidelines. Likewise, s 29(b), which provides that access does not have to be granted where doing so “would have an unreasonable impact on the privacy of other individuals”, is in the same terms as UPP 9.1(c), except that it too contains the proviso that refusal must be in accordance with any guidelines of the Privacy Commissioner.

9.71 UPP 9.1 (d) provides that access does not have to be granted where “the request for access is frivolous or vexatious”. Sections 29(j) and (k) of HRIPA correspond with UPP 9.1(d). These subsections provide, respectively, that access does not have to be granted where “the request is of a kind that has been made unsuccessfully on at least one previous occasion and there are no reasonable grounds for making the request again”, and “the individual has been provided with access to the health

105. *Health Records and Information Privacy Act 2002* (NSW) sch 1, HPP 7(2)(a) and (b).

106. It should be noted in any event that NPP 6.1(a) only applies to personal information other than health information. NPP 6.1(b) is the principle applicable to health information, and, like s 29(a), it does not contain the requirement that the threat be “imminent”.

information in accordance with this Act and is making an unreasonable, repeated request for access to the same information in the same manner”. The phrase “frivolous or vexatious” is most likely broad enough to encompass these scenarios.

9.72 Section 29(c), like UPP 9.1(e), contains an exception for personal information that “relates to existing or anticipated legal proceedings” and “would not be accessible by the process of discovery in those proceedings”. However, s 29(c) further provides that access does not have to be granted where the information sought is “subject to legal profession privilege”. Privilege is not referred to in UPP 9.1(e).

9.73 Section 29(d) provides that there is an exemption to the need to provide access to information where doing so:

Would reveal the intentions of the private sector person in relation to negotiations, other than about the provision of a health service, with the individual in such a way as to expose the private sector person unreasonably to disadvantage.

Once again, this section is similar to its equivalent, UPP 9.1(f), except that UPP 9.1(f) exempts information in circumstances where:

Providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations.

9.74 Section 29(h) states that access does not have to be given in circumstances where “providing access would be likely to prejudice a law enforcement function by or on behalf of a law enforcement agency”. UPP 9.1(j) also deals with circumstances in which access can be denied where proceedings of a law enforcement agency could be prejudiced. However, it lists the circumstances explicitly. Section 29(i) is in the same terms as UPP 9.1(k). Both provisions authorise the refusal of access to personal information upon the request of a law enforcement agency “on the basis that providing access would be likely to cause damage to the security of Australia”.¹⁰⁷

9.75 **Intermediaries.** As mentioned above, s 29(a) of HRIPA provides that access to personal information need not be granted in circumstances where it would pose a threat to the life or health of any individual.

107. *Health Records and Information Privacy Act 2002* (NSW) s 29(i); *Privacy Act 1988* (Cth) sch 3 cl 6.1(k).

Section 30 provides that, if access is refused on this ground, the individual requesting the information “may request the private sector person to give access to the information to a registered medical practitioner nominated by the individual”.¹⁰⁸ The request to give access to a registered medical practitioner must be made within 21 days of the receipt of notification that access has been refused.¹⁰⁹ The notice that access has been refused must advise the individual that he or she can ask for the information to be given to a registered medical practitioner, and also advise the individual of the time limit that applies to the making of such a request.¹¹⁰

9.76 UPP 9.3 is broader than s 30, in that it allows for the information to be given to “a mutually agreed intermediary”. It might be the case, however, that private sector health care providers will only agree to intermediaries who are registered medical practitioners. UPP 9.3 also does not include the procedural requirements contained in s 30. Presumably, such matters will be covered in OPC guidelines.

9.77 ***Procedure for accessing health information.*** Division 3 of HRIPA also deals with the procedural aspects of access to health information. For example, s 27(1) states “a private sector person must respond to a request for access within 45 days after receiving the request”. UPP 9.1, on the other hand, provides that organisations must respond to requests for access “within a reasonable time”. While this is open to interpretation, and 45 days may be considered by some longer than reasonable and others shorter than reasonable, it is an appropriate phrase to use in high level principles. Regulations could be passed to specify the time more precisely at the local level.

9.78 In relation to fees, s 27(4) specifies that access does not have to be given until seven days after any fee that arises is paid, provided that written notice of the need to pay the fee has been given within 45 days of receiving the request. UPP 9 does not contain an equivalent provision. This is appropriate in high level principles and should be a matter for guidelines or regulations at a local level.

9.79 Division 3 of HRIPA is far more prescriptive than UPP 9, which once again is appropriate, as UPP 9 is intended to be “high level” in

108. *Health Records and Information Privacy Act 2002* (NSW) s 30(2).

109. *Health Records and Information Privacy Act 2002* (NSW) s 30(3).

110. *Health Records and Information Privacy Act 2002* (NSW) s 30(4).

nature. Division 3 sets out procedures for making a request, such as requiring that requests for access be in writing and “sufficiently identify the health information to which access is being sought”.¹¹¹ It also contains provisions dealing with how a private sector person should respond to a request, and the form in which access should be provided.¹¹² If UPP 9 is adopted into NSW legislation, these procedural matters could, once again, be appropriately governed by regulations.

CORRECTION

UPP 9

9.80 In relation to correction, UPP 9 provides as follows:

9.6 If an agency or organisation holds personal information about an individual that is, with reference to a purpose for which it is held, misleading or not accurate, complete, up-to-date and relevant, the agency or organisation must take such steps, if any, as are reasonable to:

- (a) correct the information so that it is accurate, complete, up-to-date, relevant and not misleading; and
- (b) notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

9.7 If an individual and an agency or organisation disagree about whether personal information is, with reference to a purpose for which the information is held, misleading or not accurate, complete, up-to-date or relevant and:

- (a) the individual asks the agency or organisation to associate with the information a statement claiming that the information is misleading or not accurate, complete, up-to-date or relevant; and
- (b) where the information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has

111. *Health Records and Information Privacy Act 2002* (NSW) s 26(1)(a) and (b).

112. *Health Records and Information Privacy Act 2002* (NSW) s 27 and 28.

been made under the applicable provisions of a law of the Commonwealth;

the agency or organisation must take reasonable steps to do so.

Current Commonwealth law

Personal information held by agencies

9.81 Principle 7 deals with the correction of personal information held by agencies. It provides as follows:

Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:
 - (a) is accurate; and
 - (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.
2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.
3. Where:
 - (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
 - (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth.
 - (c) The record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

9.82 The ability to request that personal information be corrected or amended as set out in Principle 7 is, like the ability to access personal

information in Principle 6, also subject to other applicable laws of the Commonwealth, as Principle 7.2 demonstrates. Once again, the most pertinent piece of legislation is the FOI Act (Cth), Part V of which sets out provisions regulating the amendment and annotation of personal information held by Commonwealth agencies. The Commonwealth Privacy Commissioner’s Principle guidelines recommend that most applications for correction should, similarly to those for access, be dealt with under Part V of the FOI Act (Cth).¹¹³ However, as the Guidelines note, there are three distinctions between the correction rights available under Principle 8 and those available under the FOI Act (Cth):

1. Section 48 of the FOI Act (Cth) provides that amendment is only possible where access to the document has been “lawfully provided”. The Privacy Act is subject to this requirement but does contain a provision allowing annotation of information on a discretionary basis.¹¹⁴
2. Principle 7.1(a) allows for correction of information that is not relevant “to the purpose for which the information was collected”. Relevance is not a criteria for correction under s 48 of the FOI Act (Cth).
3. Principle 7.1 allows for correction of information to take place by way of deletion. The FOI Act (Cth) only allows for annotation or amendment.¹¹⁵

Personal information held by organisations

9.83 NPP 6.5 and NPP 6.6 regulate the correction of information held by organisations. In contrast to Principle 7, which places an obligation upon

113. Office of the Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4-7* (1988) 18 «http://www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_15.7.pdf» at 26 March 2009.

114. *Freedom of Information Act 1982* (Cth) s 48. Section 35 of the *Privacy Act 1988* (Cth) sets out a procedure via which, in circumstances where an individual has had both a request for access under the *Freedom of Information Act* and a subsequent request for amendment refused, the Privacy Commissioner can direct the relevant agency “to add to the document an appropriate notation setting out the particulars of the amendments of the document that the Commissioner thinks should be made”.

115. *Freedom of Information Act 1982* (Cth) s 48; *Privacy Act 1988* (Cth) s 14, Principle 7.1.

agencies to ensure that personal information is correct, NPP 6.5 provides that an organisation only has to correct information where an individual can show that it “is not accurate, complete and up-to-date”. The organisation must then take steps to render it so.¹¹⁶ NPP 6.6, similarly to Principle 7.3, refers to circumstances in which the individual and the organisation are unable to agree as to the accuracy of personal information. It provides that, where this situation arises, the organisation “must take reasonable steps” to “associate with the information a statement claiming that the information is not accurate, complete or up-to-date”.¹¹⁷

How and why is UPP 9 different from current Commonwealth law relating to the correction of personal information?

9.84 As noted in para 9.15 the ALRC proposed in DP 72 both the repeal of Part V of the FOI Act (Cth) and the addition to the Privacy Act of a new part dealing with access to, and correction of, personal information.¹¹⁸ The ALRC suggested that the proposed new part of the Privacy Act maintain “the same obligations that are provided for under [Principle 7]”.¹¹⁹ The ALRC further proposed that the new part of the Privacy Act state the procedures to be followed when correction is to take place, including the making of an application for correction, the time within which an agency must respond to the application, and how corrections are to be made.¹²⁰ The access and correction UPP as formulated in DP 72 was initially only to apply to organisations.¹²¹

9.85 The reasons why the ALRC moved away from this position in its final report to recommend that UPP 9 apply to both agencies and organisations are explained earlier in this chapter.¹²²

9.86 One of the main differences between the provisions of UPP 9 that relate to correction and the current Commonwealth law is that the limitations on correction of personal information held by agencies that

116. *Privacy Act 1988* sch 3, cl 6.5.

117. *Privacy Act 1988* (Cth) sch 3, cl 6.6.

118. ALRC DP 72 Proposal 12-6.

119. ALRC DP 72 vol 1 [12.51].

120. ALRC DP 72 see Proposal 12-11 (a)-(g).

121. ALRC DP 72 Proposal 26-1.

122. See para 9.17-9.18.

exist in the FOI Act (Cth) will no longer apply to applications for correction made under the Privacy Act. However, this is not the only variation from existing Commonwealth law made by UPP 9. What follows is a discussion of UPP 9.6 and UPP 9.7, and how these principles differ from both the DP 72 proposals and the current Commonwealth law.

UPP 9.6 – Removal of FOI limitations on the correction of personal information

9.87 Unlike Principle 7, which states that the obligation of agencies to correct the personal information they held is “subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents”, UPP 9.6 contains no reference to relevant Commonwealth law. In Report 108, the ALRC stated that the ability to correct information under the Privacy Act “should no longer be subject to the limitations that exist” in the FOI Act (Cth).¹²³ These limitations, discussed in detail below, can be summarised as follows:

- The individual must have been lawfully provided with the document.
- The document must have been used for an administrative purpose.
- The application must comply with procedural steps.

9.88 ***The “lawful provision” requirement.*** Section 48 of the FOI Act (Cth) provides that access to a document must be “lawfully provided”, whether under the FOI Act (Cth) “or otherwise”, before a person is entitled to ask that any errors in it be corrected. In DP 72, the ALRC suggested that the proposed new access and correction part of the Privacy Act should not contain this limitation.¹²⁴ The OPC agreed in its submission to DP 72 that “lawful access” should not be a precondition of correction.¹²⁵

123. ALRC Report 108 vol 1 [15.53].

124. ALRC DP 72 vol 1 [12.55] and Proposal 12-9. The ALRC also pointed out that, in a previous report, it had made a recommendation that the “lawful access” requirement should be removed from the FOI Act (Cth) itself: see Australian Law Reform Commission and the Administrative Review Council, *Open Government: a review of the federal Freedom of Information Act 1982*, Report No 77 (1995) Recommendation 77, as cited in DP 72 vol 1 [12.53].

125. Office of the Federal Privacy Commissioner, *Submission PR 499* (20 December 2007), as cited by ALRC Report 108 vol 1 [15.58].

9.89 The OPC noted that, if an error came to light by other means, for example, a person might be sent “a letter containing incorrect personal information”, that person should not have to go through an application process simply to request correction details they already know to be incorrect.¹²⁶ The ALRC also suggested that there might be cases where a person is denied access to a document that falls within one of the exemptions, “but they are sufficiently aware” of its contents “to know or suspect that it contains false or inaccurate information”.¹²⁷

9.90 In making the recommendation not to include this limitation in UPP 9.6, the ALRC acknowledged that “regulators and law enforcement agencies” feared that its removal could allow a person who was “the subject of current enforcement action at any stage of that process to demand correction of personal information held by the agency”.¹²⁸ The ALRC pointed out, however, that UPP 9.6 only required agencies to “take such steps, if any, as are reasonable”¹²⁹ to correct information, and “what is reasonable would depend on the circumstances in question”.¹³⁰

9.91 **Administrative purpose requirement.** Section 48(b) of the FOI Act (Cth) provides that a person can only ask for correction of information “that has been used, is being used or is available for use by the agency or Minister for an administrative purpose.” As to the meaning of “administrative purpose”, *Slezankiewicz v Australian and Overseas Telecommunications Corporation* held that this is “a purpose that has to do with the management of the agency in whose possession a document is held”.¹³¹ In Report 108, the ALRC stated that while it “did not recommend that this limitation apply” to UPP 9, it considered that “agencies should not be required to correct information that will not be used or disclosed”.¹³²

9.92 **Procedural requirements.** Sections 48-49 provide that applications for amendment must be in writing, must specify both the document

126. Office of the Federal Privacy Commissioner, *Submission PR 499* (20 December 2007), as cited by ALRC Report 108 vol 1 [15.58].

127. ALRC Report 108 vol 1 [15.61].

128. ALRC Report 108 vol 1 [15.62].

129. UPP 9.6.

130. ALRC Report 108 vol 1 [15.62].

131. *Re Tadeusz Slezankiewicz and Australian and Overseas Telecommunications Corporation* [1992] AATA 204, [46].

132. ALRC Report 108 vol 1 [15.63].

containing the record and the nature of the amendment sought and must be sent by post or delivered to the agency.¹³³ Section 50 outlines the ways in which a document can be amended by an agency where it is satisfied that amendment is justified.¹³⁴

9.93 As explained above, the OPC Guidelines advise agencies to use the procedure set out in Part V. This is because the FOI Act (Cth) and internal agency FOI policies already provide “detailed guidelines” for the processing of applications, and so using them avoids duplication. The guidelines note that this advice “is a matter of good administration, rather than a legal obligation”.¹³⁵ The ALRC recommended that the OPC should formulate guidelines on the access and correction principle, including on procedural matters.¹³⁶

Other ways in which UPP 9.6 is different from current Commonwealth law

9.94 **“Correct” information.** In Report 108, the ALRC noted “whether information is ‘correct’ for the purposes of the Privacy Act is not necessarily self-evident. Rather, this will depend upon the criteria by which correctness of personal information is assessed”.¹³⁷ The criteria contained within Principle 7 are different from those within NPP 6.5. Both principles refer to the need to ensure that information is “accurate”, “up-to-date” and “complete”, but Principle 7 states that it also must be “relevant” and “not misleading”.¹³⁸ In addition, unlike NPP 6.5, Principle 7 provides that these criteria are to be considered “having regard to the purpose for which the information was collected or is to be used and to any purpose related to that purpose”.¹³⁹

9.95 The ALRC noted that there was a “close relationship” between the “correction criteria” contained within the access and correction principles and the obligation placed upon organisations by NPP 3, the “Data Quality” principle to:

133. *Freedom of Information Act 1982* (Cth) s 48-49.

134. *Freedom of Information Act 1982* (Cth) s 50.

135. Office of the Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4-7*(1998) <http://www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_15.7.pdf 18> at 26 March 2009.

136. ALRC Report 108 vol 2 Recommendation 29-9.

137. ALRC Report 108 vol 2 [29.89].

138. *Privacy Act 1988* (Cth) s 14, Principle 7 and sch 3, cl 6.5.

139. *Privacy Act 1988* (Cth) s 14, Principle 7.

Take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

At the moment, agencies are not subject to a separate data quality principle, although some principles include similar elements as the data quality principle.¹⁴⁰ The ALRC has devised a model ‘Data Quality’ UPP that will apply to agencies as well.¹⁴¹

9.96 In DP 72, the ALRC proposed that UPP 9, which was only to apply to organisations at that stage, should provide that an individual who sought correction of personal information held by an organisation must show that the information was “with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant”.¹⁴² This proposal was designed to bring the ‘Access and Correction’ principle into line with the data quality principle.¹⁴³ The ALRC also proposed that a like obligation for agencies should be included in the proposed new Part of the Privacy Act.¹⁴⁴

9.97 In Report 108, the ALRC noted that most of the submissions it received supported these proposals, although some raised concerns as to whether the requirement to have reference to purpose of collection might enable an organisation to refuse to correct information that might be incorrect in relation to one purpose, but correct for another.¹⁴⁵ The ALRC also noted that Privacy NSW supported the proposed change in relation to agencies, but said that this was “provided the existing provisions of the FOI Act are referred to in the ‘Access and Correction’ principle itself, or that it is annexed to the Privacy Act”.¹⁴⁶ The Australian Communications and Media Authority expressed concern that this proposal could have implications for both agency resources and the capacity for some agencies to carry out their regulatory or law enforcement functions.¹⁴⁷

9.98 The ALRC ultimately expressed the view that a person “should be provided with the right to correct personal information held by agencies

140. ALRC Report 108 vol 2 [29.94], see Principles 3, 8 and 7.

141. The Data Quality Principle is UPP 7, and is discussed in detail in Chapter 7.

142. ALRC DP 72 Proposal 26-5.

143. ALRC Report 108 vol 2 [29.95].

144. ALRC DP 72 Proposal 12-9(a).

145. ALRC Report 108 vol 2 [29.97].

146. ALRC Report 108 vol 2 [29.98].

147. ALRC Report 108 vol 2 [29.98].

and organisations where the information is misleading or not accurate, relevant, up-to-date or complete”.¹⁴⁸ The ALRC noted that the data quality principle already obliged agencies or organisations holding irrelevant personal information “to destroy it, or render it non-identifiable” in most situations.¹⁴⁹ The ALRC further noted that it might be possible for “an agency or organisation to hold personal information that is relevant for one of its functions or activities but not another”. In such cases, the ALRC suggested, the individual should be able to have the information corrected in relation to the purpose for which it is irrelevant.¹⁵⁰

9.99 As the discussion above demonstrates, the ALRC did not propose in DP 72 that the criteria of “misleading” should be applied to organisations in DP 72. However, in Report 108 the ALRC noted that, under s 18J of the Privacy Act, credit reporting agencies were required to ensure that personal information in credit information files and credit reports was not misleading.¹⁵¹ Furthermore, the ALRC did not believe that imposing a requirement upon organisations to correct information that was misleading “would impose a significant new compliance burden upon” them.¹⁵² It noted that often information that was “misleading” would fall under one of the other categories of information requiring correction anyway.¹⁵³

9.100 The ALRC noted that, in circumstances where “information is ‘misleading’, but is otherwise accurate, complete, up-to-date and relevant, this will result in a difference between the correction requirements of the ‘Access and Correction’ principle and the ‘Data Quality’ principle”. The ALRC indicated, however, that since these principles operated in “different contexts”, it considered “this discrepancy to be appropriate”.¹⁵⁴

9.101 Also in relation to data quality, the ALRC observed that it should be measured, in accordance with the data quality principle, “with reference to the purpose for which [the] information is being collected,

148. ALRC Report 108 vol 2 [29.99].

149. ALRC Report 108 vol 2 [29.100].

150. ALRC Report 108 vol 2 [29.100].

151. ALRC Report 108 vol 2 [29.101].

152. ALRC Report 108 vol 2 [29.101].

153. ALRC Report 108 vol 2 [29.101].

154. ALRC Report 108 vol 2 [29.102].

used or disclosed”.¹⁵⁵ However, where the access and correction principle is engaged, whether or not information is correct “should be ascertained by reference to the purpose for which information is being held”.¹⁵⁶ The ALRC noted that, when it is being considered whether or not personal information is correct in accordance with UPP 9, “[t]he purpose justifying retention of the information under the ‘Data Security’ principle also should be taken into account”.¹⁵⁷

9.102 ***Establishing that personal information is not correct.*** NPP 6.5 places an obligation on individuals requesting corrections to personal information to “establish that the information is not accurate, complete and up to date”. Under Principle 7.1, however, the obligation rests with an agency to ensure that personal information it holds is correct. The ALRC did not suggest the removal of the onus in NPP 6.5 in DP 72, but it nonetheless received submissions stating that the onus led to uncertainty, since the principle itself did not contain any indication of the standard of proof to which an individual should be held when attempting to establish the inaccuracy of the information.¹⁵⁸

9.103 The ALRC accepted these submissions. As a result, the proposed UPP 9.6 requires agencies and organisations to ensure that their records are correct “in accordance with the requisite criteria”.¹⁵⁹ The form of the words used is similar to that of Principle 7.1. The ALRC noted that since agencies are already subject to this obligation, they should not have to alter their existing practices.¹⁶⁰ The ALRC further noted that this change should not overly affect the practices of organisations. It will remain necessary for an individual seeking correction of information to show that it is incorrect, or for the agency or organisation to demonstrate that it is correct.¹⁶¹ However, the ALRC stated that, where a complaint arises about a decision in relation to UPP 9.6, “the relevant issue is the

155. ALRC Report 108 vol 2 [29.104], see also UPP 7.

156. ALRC Report 108 vol 2 [29.104].

157. ALRC Report 108 vol 2 [29.105].

158. ALRC Report 108 vol 2 [29.107]-[29.108].

159. ALRC Report 108 vol 2 [29.110].

160. ALRC Report 108 vol 2 [29.110].

161. ALRC Report 108 vol 2 [29.110].

correctness of the personal information that is held by the agency or organisation”.¹⁶²

9.104 ***How correction should be carried out.*** NPP 6 contains no mention of how correction should be carried out. Principle 7.1 provides that, when correcting personal information, an agency must make “appropriate corrections, deletions and additions as are in the circumstances reasonable” in order to ensure the accuracy of the record. Section 50(3) of the FOI Act (Cth) further provides that, when an agency is amending personal information, it must, “to the extent that it is reasonably practical to do so”, make sure “that the record of information is amended in a way that does not obliterate the text of the record as it existed prior to the amendment”. If UPP 9 is accepted, the form of an application to correct personal information under the Privacy Act will not be subject to this FOI requirement.

9.105 The ALRC stated, that while no proposal in DP 72 addressed this issue in particular, it received some submissions that “noted the potential tension between the obligation to correct personal information and archiving responsibilities”.¹⁶³ The ALRC noted the submission of the National Archives of Australia, which expressed concern regarding any potential changes to the FOI Act (Cth) that might promote the deletion of personal information at the expense of other requirements of proper record-keeping. The National Archives submitted that, rather than deleting information, it was more appropriate to amend or correct a record.¹⁶⁴

9.106 The ALRC concluded that the issue of how to balance the need to correct personal information with record-keeping obligations, such as those under the *Archives Act 1983* (Cth), should be covered in the guidelines on UPP 9 it had recommended that the OPC produce.¹⁶⁵

Notifying third parties

9.107 UPP 9.6(b) provides that, when a correction is made to personal information, an “agency or organisation must take such steps, if any, as are reasonable” to:

162. ALRC Report 108 vol 2 [29.110].

163. ALRC Report 108 vol 2 [29.114].

164. ALRC Report 108 vol 2 [29.115], citing the submission of the National Archives of Australia, *Submission PR 414*, 7 December 2007.

165. ALRC Report 108 vol 2 [29.116].

Notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practical in the circumstances.

This requirement does not appear in either NPP 6 or Principle 7. However, the ALRC noted that record-holders in other jurisdictions, for example, Canada and Germany, were required to notify third parties when correction of personal information had taken place.¹⁶⁶ In DP 72, the ALRC proposed that the new part of the Privacy Act should contain a provision directing agencies to notify third parties of the correction of information, where they were requested to do so by an individual.¹⁶⁷ The ALRC also proposed that organisations should be subject to a similar requirement under UPP 9.¹⁶⁸

9.108 The ALRC received a number of submissions on this point. Some supported the inclusion of this requirement. Some suggested that it be widened, for example, by removing the need for an individual to request notification of third parties.¹⁶⁹ However, other submissions expressed concern at the proposal, and indicated that it could have resource implications for both agencies and organisations.¹⁷⁰ Further submissions argued that it placed an “inappropriate burden” on agencies and organisations.¹⁷¹

9.109 The ALRC quoted from the submission by GE Money Australia, which pointed out that the proposal “appears to have implicit in it that there is a fault on the part of the organisation by reason of it having and having disclosed information that may not be correct or up to date” when it might be the case that the information provided to the organisation itself might have been “[i]ncorrect or unclear”.¹⁷² The ALRC also quoted the submission made by ANZ to the effect that, while it did not think the change was necessary, if the requirement to notify third parties was included in UPP 9 it should be qualified only to apply “where

166. ALRC Report 108 vol 2 [29.121].

167. ALRC DP 72 Proposal 12-9(b).

168. ALRC DP 72 Proposal 26-4.

169. ALRC Report 108 vol 2 [29.126].

170. ALRC Report 108 vol 2 [29.127].

171. ALRC Report 108 vol 2 [29.128].

172. GE Money Australia, *Submission PR 537*, 21 December 2007, as cited in ALRC Report 108 vol 2 [29.128].

inaccuracies are considered by a reasonable person to be material and [notification] would be practical in the circumstances”.¹⁷³

9.110 The ALRC concluded that the requirement should be included in order to “reduce the risk that any entities to which the incorrect personal information has been disclosed will use or disclose the information inappropriately at a later time”.¹⁷⁴ The ALRC was of the opinion that the “reasonable steps” qualification contained within UPP 9.6(b) should help to address the concerns about the cost burden that this requirement might place on agencies and organisations.¹⁷⁵ The ALRC indicated that the OPC give guidance as to what factors an agency or organisation should consider when determining whether it was “reasonable and practicable to notify third parties that it has disclosed incorrect information”.¹⁷⁶

UPP 9.7 – Annotation of personal information

9.111 Principle 7.3 provides that, where an agency does not agree to correct personal information:

[T]he record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable to attach to the record any statement provided by the individual of the correction, deletion or addition sought.

9.112 In similar circumstances, NPP 6.6 directs an organisation to “take reasonable steps” to “associate” with disputed information a statement that it “is not complete, accurate or up-to-date” if the individual in question so requests.

9.113 In DP 72, the ALRC stated that, in its view, the word “associate”, used in NPP 6.6, was more appropriate than the word “attach,” which was used in Principle 7.3, since it was “more technologically neutral, allowing a more flexible approach for organisations that record personal information electronically”.¹⁷⁷ The ALRC believed that the word “associate” was, as a result, “more likely to achieve the main objective” of this principle, which was to “ensure that the opinion of the individual

173. ANZ, *Submission 467*, 13 December 2007, as cited in ALRC Report 108 vol 2 [29.129].

174. ALRC Report 108 vol 2 [29.130].

175. ALRC Report 108 vol 2 [29.131].

176. ALRC Report 108 vol 2 [29.132], see also Recommendation 29-9.

177. ALRC DP 72 vol 2 [26.37].

concerned is easily accessible when the organisation seeks to use or disclose” the information.¹⁷⁸

9.114 The ALRC received submissions in support of this proposal.¹⁷⁹ It concluded that UPP 9.7(a), which was now to apply to both agencies and organisations,¹⁸⁰ should contain the word “associate” rather than “attach.” The ALRC considered that it was “inherent to the meaning of ‘associate’” that statements were associated in a way that makes them “apparent to subsequent users”.¹⁸¹

9.115 UPP 9.7(b), which is applicable to agencies only, contains a qualification of the above requirement to associate a statement where so requested. The agency is to do so:

Where no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth.

9.116 This is in the same terms as Principle 7.3(b). The ALRC concluded that this proviso should continue to apply while Part V of the FOI Act (Cth) remains in operation. In addition, the ALRC stated that s 35 of the Privacy Act should also be retained. This section grants the Privacy Commissioner power to direct an agency to amend a document where an application for amendment has been made under s 55(1) of the FOI Act (Cth) and the agency has refused to comply with the request. The ALRC noted that s 35 “compliments the limitation under [Principle] 7.3”.¹⁸² The ALRC further commented that:

These provisions would not be required if the FOI Act did not regulate the correction of personal information. These provisions should be considered as part of the ALRC’s review of the FOI Act and related laws.¹⁸³

178. ALRC DP 72 vol 2 [26.37].

179. ALRC Report 108 vol 2 [29.136].

180. See para 9.19.

181. ALRC Report 108 vol 2 [29.137].

182. ALRC Report 108 vol 2 [15.69].

183. ALRC Report 108 vol 2 [15.70].

Current NSW law

9.117 IPP 8 (s 15, PPIPA) deals with the correction or “alteration” of personal information. It provides that, following a request from an individual about whom a public sector agency holds information, the agency must, at the request of an individual, make any amendments that may be necessary to ensure that the information:

- (a) is accurate, and
- (b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.¹⁸⁴

9.118 In circumstances where an agency refuses to alter information in accordance with a request, the individual making the request may provide the agency with a statement describing the amendment requested and ask that the agency attach the statement to the information “in such a manner as is capable of being read with” it.¹⁸⁵ IPP 8(3) further provides that, where information is amended by an agency, the individual requesting the amendment “is entitled, if it is reasonably practicable” to have “recipients” of the information be informed of the amendments made to it.

9.119 Like the FOI Act (Cth), the FOI Act (NSW) sets out a procedure, contained within Part 4, for the amendment of personal records. Section 39 of the FOI Act (NSW) provides that a person can “apply for the amendment of the agency’s records” in circumstances where they contain “information concerning that person’s affairs”, are used by the agency “in connection with its administrative functions” and the information in them is “in the person’s opinion, incomplete, incorrect, out of date or misleading”. Part 4 also sets out a procedure for dealing with applications, and one for annotating records in circumstances where applications for amendment are refused. As is the case with access to personal information, the FOI Act (NSW) is far more prescriptive in relation to how correction is to take place than PPIPA. Under Schedule 1 of the *Government Information (Consequential Amendments and Repeals) Act*

184. *Privacy and Personal Information Protection Act 1998* (NSW) s 15(1), IPP 8(1).

185. *Privacy and Personal Information Protection Act 1998* (NSW) s 15(2), IPP 8(2).

2009 (NSW), Part 4 of the FOI Act (NSW) is being moved temporarily to PPIPA.¹⁸⁶

Health information

9.120 HPP 8(1), (2) and (3) of HRIPA is drafted in the same terms as IPP 8(1), (2) and (3). Once more, the only difference is that HPP 8 applies to private sector health care providers as well as public sector ones. A statutory note in HPP 8 states that amendment in relation to information held by public sector organisations may also be sought under the FOI Act (NSW), while Division 4 of Part 4 of HRIPA contains provisions relevant to the amendment of private sector-held information. Division 4 of Part 4 sets out a procedure for the making and resolution of applications for amendment of health information. A further statutory note in Division 4 indicates that its provisions are “additional to, and assist the operation of, the general principles in HPP 8”.¹⁸⁷ Section 35 of HRIPA deals with annotation of the record in circumstances where the “private sector person” has refused to correct it.

NSWLRC Consultation Paper 3

9.121 Apart from the issues discussed at the outset of this chapter,¹⁸⁸ the only other issue raised by the Commission in CP 3 in relation to correction was to do with an apparent inconsistency between sub-sections (1) and (2) of s 15 of PPIPA (IPP 8). Subsection 15(1) provides that an agency must amend personal information if requested, whereas s 15(2) provides that, if the agency is not prepared to make amendments as requested, then certain steps follow. In other words, s 15(2) envisages that the agency can refuse to make requested amendments, whereas s 15(1) is apparently making an amendment mandatory upon request.

9.122 This issue does not have a bearing on UPP 9, which avoids the inconsistency. Like s 15(1), UPP 9.6 places an obligation on an agency (or organisation) to correct information but, unlike s 15(2), UPP 9.7 departs from the obligation only where the agency/organisation doesn't agree that there is an inaccuracy, or suchlike.

186. See para 9.5.

187. *Health Records and Information Privacy Act 2002* (NSW) Part 4, Division 4, statutory note.

188. See para 9.8-9.11.

How is NSW law different from the proposed UPP 9?

FOI limitations

9.123 As discussed above, it is not clear exactly which provisions of the FOI Act (NSW) are imported into PPIPA by s 20(5), or into HRIPA by s 22(3).¹⁸⁹ Section 39 of the FOI Act (NSW) refers to the “right to apply for amendment of agencies, records”. If this is read in the same way as s 48 of the FOI Act (Cth),¹⁹⁰ it contains two limitations that are not in UPP 9. We agree in principle that the limitations should not apply to requests for correction of personal information.

Other changes

9.124 In NSW, both IPP 8 and HPP 8 state that the agency or private sector health care provider must “make appropriate amendments” to the personal information they hold “at the request of the individual to whom the information relates”. Hence, unlike UPP 9.6, IPP 8 and HPP 8 refer specifically to the need for the individual to request correction before it takes place. However, also unlike NPP 6.5 the NSW principles do not place a burden of proof upon the individual to show that the information is incorrect. This differs from UPP 9.6, which places an obligation upon agencies and organisations to correct personal information that is incorrect, but does not specifically anchor this obligation to a request from the individual. UPP 9.6 also differs from NPP 6.5, which, as explained above stated that information had to be corrected where an “individual is able to establish” that it is incorrect.

9.125 In relation to the criteria against which personal information is to be assessed as correct or not, the current NSW principles state that information should be “accurate” and “having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading”. These criteria reflect those in UPP 9.6. Indeed the changes to the Commonwealth law recommended by the ALRC bring the UPP more closely in to line with the NSW correction principles. If not prepared to amend information in accordance with a request for correction, both IPP 8 and HPP 8 provide that agencies and private health care providers must:

189. See para 9.8-9.10.

190. See para 9.88-9.90. The Commission is not persuaded that this is the correct interpretation of s 39.

[T]ake such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

9.126 The decision by the ALRC to use the word “associate” rather than “attach” in circumstances where an individual has requested that a statement of desired changes be affixed to a record that an agency or organisation has refused to change, and the policy reasons which underlie this decision, also brings the UPP into line with NSW correction principles.¹⁹¹

9.127 In relation to the need to notify third parties of changes, IPP 8(3) provides:

If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the public sector agency.

9.128 HPP 8(3) contains the same requirement. Therefore, NSW agencies and private sector health care providers are already under an obligation to notify third parties of corrections made to the personal information of an individual. Like the obligation in UPP 9.6(b), this is to occur upon the request of the individual who sought correction of the information and in circumstances where it is “reasonably practicable”.¹⁹² Furthermore, under HRIPA, private health care providers are not only required to notify third parties of corrections they have made to information. Section 35(3) of HRIPA places a further obligation on the private health care provider to ensure that, in circumstances where a request for correction has been refused and a notation added to the record, it must give any third party to which the information in question is disclosed a statement indicating that the individual does not think the information is correct and also

191. However it should be noted that s 35 of the *Health Records and Information Privacy Act 2002* (NSW) simply provides that the private sector person should “add a notation” to the information. Section 46 of the *Freedom of Information Act 1989* (NSW) also just requires that the notation be added, without specifying how.

192. *Privacy and Personal Information Protection Act 1998* (NSW) s 15, IPP 8, UPP 9.6(b) provides that notification is to take place upon request and where it “would be practicable in the circumstances”.

setting out the particulars of any notation that has been added to the information.¹⁹³

9.129 Unlike IPP 8(3), HPP (3) also includes a Statutory Note that provides that correction of health information held by agencies may also be sought under the FOI Act (NSW), and also that Division 4 of Part 4 of HRIPA “contains provisions applicable to private sector persons in connection with the matters dealt with in this clause”. Division 4 of Part 4 of HRIPA sets out the procedure that private sector health care providers must follow in relation to requests for amendment of personal information. It also covers such matters as the form a request should be in and the timeframe in which the private sector health care provider should respond, and provides for the annotation of records in circumstances where the health care provider does not agree that the information is incorrect.¹⁹⁴

REFUSAL OF REQUEST TO ACCESS OR CORRECT

UPP 9

9.130 Where an agency or organisation refuses to provide access to or correct personal information, UPP 9.8 provides:

- 9.8 Where an agency or organisation denies a request for access or refuses to correct personal information it must provide the individual with:
- (a) reasons for the denial of access or refusal to correct the information, except to the extent that providing such reasons would undermine a lawful reason for denying access or refusing to correct the information; and
 - (b) notice of potential avenues for complaint.

193. *Health Records and Information Privacy Act 2002* (NSW) s 35(3). The *Freedom of Information Act 1989* (NSW) also contains a like provision, s 46(3), but this only applies to applications for correction made under the *Freedom of Information Act 1989* (NSW) itself. This section is not applicable where an individual makes a request to an agency under the *Privacy and Personal Information Protection Act 1998* (NSW).

194. *Health Records and Information Privacy Act 2002* (NSW) s 33-35.

How UPP 9.8 is different from current Commonwealth law

9.131 NPP 6.7 provides that organisations “must provide reasons for denial of access or a refusal to correct personal information”, but NPP 6 does not contain any reference to a need to provide notice of potential avenues of complaint. There is no requirement in Principles 6 or 7 to give either reasons or notice of avenues of complaint. However, s 26 of the FOI Act (Cth) requires a “decision-maker” to “cause the applicant to be given notice in writing of the decision”.¹⁹⁵ Section 26 also specifies that the notice should:

[S]tate the findings on any material questions of fact, referring to the material on which those findings were based, and state the reasons for the decision.¹⁹⁶

Under s 26(1)(c), the notice should also “give to the applicant information concerning” his or her right to have the decision reviewed or complain to the Ombudsman, and also set out the procedure for the exercise of either of these rights.¹⁹⁷

9.132 The ALRC noted that, although no proposal was put forward on this issue in DP 72, it received some submissions on the matter.¹⁹⁸ The ALRC said that “[p]rivacy advocates submitted that the obligation to give reasons needed to be more specific in requiring an organisation to specify *which* of the exemptions it has relied on to deny access or correction”.¹⁹⁹ The ALRC also stated that the Commonwealth Attorney-General’s Department had submitted that “there should be an exception from the requirement to provide a reason for denial of access where the reason for denial is because of one or more of paragraphs 9.1(f) to (j) of the proposed ‘Access and Correction’ principle” because providing reasons for not granting access “may prejudice investigations or prosecutions in relation to mutual assistance or extradition”.²⁰⁰ In addition, the Office of the Victorian Privacy Commissioner submitted that organisations that have

195. *Freedom of Information Act 1982* (Cth) s 26.

196. *Freedom of Information Act 1982* (Cth) s 26(1)(a).

197. *Freedom of Information Act 1982* (Cth) s 26(1)(c).

198. ALRC Report 108 vol 2 [29.171].

199. ALRC Report 108 vol 2 [29.172], italics, in the original.

200. ALRC Report 108 vol 2 [29.173].

refused access to personal information “should be required to advise individuals about how this decision can be appealed”.²⁰¹

9.133 The ALRC concluded that, where an agency or organisation has decided to refuse a request for access or correction, “it is an important element of procedural fairness for the individual to be provided with the reason for the adverse decision”.²⁰² In its view, this would generally “require the agency or organisation to tell the individual which exception it is relying on to refuse access”.²⁰³ The ALRC noted that there might be circumstances where the provision of reasons for the decision “would undermine the very reason that the agency or organisation has denied the individual access to the information or has refused to make the requested correction”.²⁰⁴ The ALRC recommended that UPP 9 should provide for this contingency.²⁰⁵

9.134 The ALRC also considered it appropriate for agencies and organisations to notify applicants of any avenues of appeal they may have in relation to the decision not to allow access or correct personal information. The ALRC recommended that this should be done in the Privacy Policy of the agency or organisation. It stated that, as long as “this Privacy Policy is readily available, it would be open to an agency or organisation to meet its requirements under the ‘Access and Correction’ principle by referring individuals to the relevant section of this document”.²⁰⁶

201. ALRC Report 108 vol 2 [29.174].

202. ALRC Report 108 vol 2 [29.175].

203. ALRC Report 108 vol 2 [29.175].

204. ALRC Report 108 vol 2 [29.176].

205. ALRC Report 108 vol 2 [29.176], Recommendation 29-8.

206. ALRC Report 108 vol 2 [29.177]. Note further on the subject of notification of access and correction rights, in DP 72, the ALRC proposed that the recommended new part of the Privacy Act should provide that “where an individual is given access to personal information, the individual must be advised that he or she may request the correction of that information” (see ALRC DP 72 Recommendation 12-8(b)). No such proposal was made in relation to organisations, although the ALRC did say in DP 72 ([26.60]) that, in its view, “the proposed ‘Specific Notification’ and ‘Openness’ principles [would] adequately cover this issue”. The ALRC received submission in support of the proposal, although it noted that ACMA expressed concern regarding possible implications for resources and law enforcement and regulatory functions of agencies. The ALRC ultimately decided that, while “[a]gencies and

How UPP 9.8 is different from NSW law

9.135 There is currently no requirement to give reasons for the refusal to allow access to, or to correct, personal information. However, Part 4 of HRIPA and the FOI Act (NSW) each contain provisions stating that, in circumstances where access or correction is refused, written reasons for the refusal should be provided by the agency or organisation.²⁰⁷ The provisions relating to reasons in the FOI Act (NSW) include detailed requirements as to what these “notices of determination” should contain. For example, s 28 of the FOI Act (NSW), which relates to decisions made in relation to the access of documents, provides that the notice shall specify the date of the determination, the reasons for the decision and “the findings on any material questions of fact underlying those reasons, together with a reference to the sources of information on which those findings are based”, as well as the name of the officer who made the determination, any rights of review available to the individual making the request for access and the procedures to be followed in exercising those rights.²⁰⁸ Section 45 contains the same requirements for notices of determination in relation to requests for correction.

9.136 If UPP 9 is adopted in NSW, it may be necessary to address any gaps in the procedural aspects of the access and correction process in guidelines issued by the NSW Privacy Commissioner.

CONCLUSION

9.137 UPP 9 goes some way towards addressing the longstanding problems that arise from the overlapping provisions of the FOI and privacy legislation. For example, the ALRC has begun to disentangle the procedure for access and correction under the privacy legislation from that under the FOI legislation, and some of the changes embodied in

organisations should take steps to inform individuals of their access and correction rights”, the Privacy Act itself did not need to include such a requirement. The ALRC indicated that UPP 3(c), which provides that agencies and organisations must notify individuals of their access and correction rights at the time their information is collected, “sufficiently encompassed” this issue (see ALRC Report 108 vol 2 [29.178]-[29.181]).

207. See *Health Records and Information Privacy Act 2002* (NSW) s 27(3) and s 34(4); *Freedom of Information Act 1989* (NSW) s 28 and 45.

208. *Freedom of Information Act 1989* (NSW) s 28, particularly s 28(e)(ii).

UPP 9 may help to simplify the actual process of accessing and correcting personal information.

9.138 However, we must return to the point made at the beginning of this chapter, which is that UPP 9 does not, and indeed cannot, entirely address the problems arising from the overlap between the Privacy Act and the FOI Act (Cth). We also reiterate our earlier point that, while access under privacy legislation remains subject to exemptions under the FOI legislation, access interests will not be uniform across jurisdictions unless the exemption provisions of Commonwealth and State FOI legislation are comparable.

9.139 At this stage, the Commission is of the view that UPP 9 is an adequate access and correction privacy principle. However, many of the questions that arise in relation to UPP 9 also raise, or relate to, issues regarding the interface between privacy and FOI legislation, and, as likewise noted in the introduction, the landscape here is changing. UPP 9 will need to be considered in the context of any future report on privacy and access to personal information.

10.

UPP 10: Identifiers

- Introduction
- ALRC Report 108
- The Commission's view

INTRODUCTION

10.1 “Identity” means “the condition of being oneself... and not another”.¹ Identifiers are the means by which we verify a person’s identity so that he or she may be identified or recognised as being a particular person.

10.2 There are many different types of identifiers depending on the particular context in which identification is required. In a social context, physical appearance and mannerisms, and knowledge of private information are some common identifiers. In business dealings, passports, birth certificates, bank cards and Medicare cards are used as identifiers unique to a particular person. Most forms of identification used for business purposes have a number allocated to the person as a unique identifier.

10.3 The main reason for allocating a unique number as an identifier is to protect privacy and reduce the possibility of criminal behaviour. This is dependent, however, on the number or code and the information it holds remaining confidential and not being widely known or accessed by the world at large. It is for this reason that the use and disclosure of identifiers should be regulated.

Current legislative regulation of identifiers

Federal legislation

10.4 Federally, the Privacy Act regulates the adoption, use and disclosure of unique identifiers by organisations through NPP 7. The Principles that regulate the activities of Australian government agencies do not contain a principle dealing explicitly with identifiers. Thus, the use of identifiers by government agencies is not regulated.

10.5 Apart from the privacy concerns that arise from the use and disclosure of unique identifiers, the use of multi-purpose identifiers (which are unique identifiers assigned to individuals for use by multiple agencies and organisations) also give rise to many privacy concerns. Their use has the potential to extend the government’s power over, and access to, a wide range of an individual’s personal information including information pertaining to financial, health and family status. The failed

1. Macquarie Dictionary, 1981, at 879 (definition 3 of 9).

Australia Card and Medicare Card schemes are examples of what may have been national identification schemes. In DP 72, the ALRC expressed the view that the access card number under the now abandoned access card scheme, may have fallen within the definition of “identifier” in the proposed Unified Privacy Principle regulating identifiers, as it was intended to regulate unique multi-purpose identifiers that were not otherwise regulated by specific legislative regimes.² In Report 108, the ALRC recommended that, before the introduction by any agencies of any unique multi-purpose identifiers, the Australian Government, in consultation with the Privacy Commissioner, should consider the need for a privacy impact assessment.³

10.6 The Tax File Number (“TFN”) Scheme⁴ is also relevant in this context, although not directly regulated by the Privacy Act. The handling of TFNs is regulated under various federal Acts.⁵ However, the ALRC has noted that s 17 of the Privacy Act enables the Privacy Commissioner to issue legally binding guidelines concerning the collection, storage, use and security of “tax file number information”.⁶ A breach of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) or its guidelines constitutes an interference with privacy under s 13 of the Privacy Act.

NSW legislation

10.7 In NSW, HRIPA, which protects the privacy of an individual’s health information in both the public and private sectors, does include an identifier principle in HPP 12. However, PPIPA, which regulates the handling of personal information (excluding health information) by NSW

2. Australian Law Reform Commission, *Review of Australian Privacy Law* Discussion Paper 72 (2007) (“ALRC DP 72”) [27.109]-[27.110].

3. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) Recommendation 27-5.

4. It was primarily designed to reduce tax evasion and makes provision for the Commissioner of Taxation to provide a TFN to any person, if satisfied of their identity. The TFN is quoted when the applicant commences employment, engages in investment activities or accesses federal income support and is used by Centrelink to match records between the Australian Taxation Office and specified assistance agencies.

5. For example, Part VA of the *Income Tax Assessment Act 1936* (Cth), the *Taxation Administration Act 1953* (Cth), the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and Guidelines under the Act regulate data matching using TFNs.

6. ALRC Report 108 vol 2 [30.136].

agencies, does not contain a provision regulating the use of identifiers. The consequence is that, in NSW, individuals whose personal information comes within the ambit of PPIPA do not have the benefit of a provision regulating identifiers. This lack of regulation exposes an individual to the danger of a third party having access to information about the individual connected with a unique identifier for unauthorised purposes. The Commission, in CP 3, was of the view that “this is an omission that needs to be rectified”.⁷

Focus of this chapter

10.8 The Commission proposed in CP 3 that NSW legislation should only apply to the handling of personal information by agencies.⁸ However, the identifier principle as set out in UPP 10 applies only to organisations. While it is arguable that there is little justification limiting regulation of identifiers to organisations when the rationale is just as capable of application to agencies, we agree with the ALRC’s reasoning for limiting overall application to organisations, while permitting a case-by-case approach to agencies.⁹ Given that NSW privacy legislation may only be applicable to agencies, and NSW organisations can be covered under Commonwealth legislation, it may not be strictly necessary to include an identifier principle within the reformed NSW privacy legislation. However, given the goal of achieving national uniformity, it is unlikely that including an identifier principle that mirrors the federal principle will be detrimental to NSW.

10.9 The aim of this chapter, therefore, is to evaluate the ALRC’s UPP 10 to ascertain whether it adequately, regulates the inherent threats to privacy and the possibility for the misuse of identifiers and whether the draft principle can be mirrored in NSW with or without modification.

ALRC REPORT 108

10.10 Before evaluating UPP 10 and its relationship to the identifier principle in HRIPA, it is useful to consider two preliminary issues. They are the ALRC’s rationale for:

-
7. NSW Law Reform Commission, *Privacy Legislation in New South Wales Consultation Paper 3 (2008)* (“NSWLRC CP 3”) [6.68].
 8. NSWLRC CP 3 Proposal 3.
 9. See para 10.20.

- a separate identifier principle; and
- excluding government agencies from the ambit of the identifier principle.

Rationale for a separate identifier principle

10.11 While the use and disclosure of information contained in identifiers is, and must continue to be, regulated, a threshold issue to be determined is whether there must be a separate identifier principle or whether regulation can be accommodated within other privacy principles that deal with collection, use and disclosure of personal information.

10.12 In determining this issue, it is useful to revert to the policy rationale for the introduction of the principle in the first place. According to the ALRC, the policy bases for the identifier principle are twofold:

First, NPP 7 was introduced to ensure that the increasing use of Australian Government identifiers does not lead to a de-facto system of universal identity numbers. Secondly, the regulation of identifiers reflects concern about the facilitation of data matching by identifiers.

10.13 The ALRC raised this issue in its Issues Paper 31 (“IP 31”)¹⁰ and received a few submissions in response. While two stakeholders were of the view that a separate principle was not required,¹¹ most others supported a separate principle.

10.14 One reason for arguing against a separate privacy principle regulating identifiers is on the basis that the collection, use and disclosure of identifiers can be accommodated within other privacy principles. For example, the proscription in NPP 7.1 against an organisation adopting as its own identifier an identifier that has been assigned by an agency, can be accommodated within the privacy principle regulating the use of personal information. Similarly, some of the exceptional circumstances when use or disclosure of an identifier is allowed are already contained in NPP 2.

10. Australian Law Reform Commission, *Review of Privacy Issues Paper 31* (2006) (“ALRC IP 31”) Question 4-26.

11. Australian Government Department of Human Services, *Submission PR 136*, 19 January 2007; Insurance Council of Australia, *Submission PR 110*, 15 January 2007, cited in ALRC DP 72 [27.15].

10.15 On the other hand, the submissions supporting retention argued that a separate principle provides “a clear principle prohibiting the development of a universal or approaching universal identifier”,¹² “performs a useful task in limiting the use of identifiers for data matching and data linkage”,¹³ and overall “serves an important function in protecting information privacy”.¹⁴

10.16 A separate privacy principle can also deal with issues specific to the principle, such as the definition of an identifier and specific exceptions to the principle. Given that there was no suggestion that accommodating the identifier principle within other privacy principles would provide a more effective way of regulating identifiers, the ALRC, in DP 72, proposed that the UPPs should contain a separate principle that regulates identifiers.¹⁵ Again, the submissions received in response to the DP were supportive of the ALRC’s proposal to have a separate privacy principle regulating identifiers. Arguing against accommodating the identifier principle within other principles such as collection, use and disclosure, one submission stated that it “would be unnecessarily complex, and would fail to give adequate recognition to the serious privacy risks associated with the misuse of identifiers”.¹⁶

10.17 Having reviewed the submissions it received, and given that the majority of the submissions to IP 31 and DP 72 did support a separate principle regulating identifiers, and in the absence of a sound argument to the contrary, the ALRC recommended that the model Unified Privacy Principles should contain a separate principle regulating identifiers.¹⁷

Rationale for excluding government agencies

10.18 The ALRC also considered the issue of whether the “identifiers” principle should be extended to apply to agencies. In DP 72, having

12. Queensland Council for Civil Liberties, *Submission PR 150*, 29 January 2007, cited in ALRC DP 72 [27.13].

13. Office of the Information Commissioner (Northern Territory) *Submission PR 103*, 15 January 2007, cited in ALRC DP 72, [27.13].

14. Office of the Privacy Commissioner, *Submission PR 215*, 28 February 2007, cited in ALRC DP 72 [27.13].

15. ALRC DP 72 Proposal 27-1.

16. Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007, cited in ALRC Report 108 [30.16].

17. ALRC Report 108 Recommendation 30-1.

considered the submissions made to IP 31,¹⁸ the ALRC proposed that the identifier principle should apply to both agencies and organisations on the basis that the policy objectives underlying the regulation of the use of identifiers in organisations equally apply to agencies.¹⁹ However, while some submissions were supportive of such extended coverage, other submissions to DP 72 expressed a contrary view and nearly all agencies were concerned about its operation.²⁰

10.19 The main justification for extending applicability to agencies is to ensure that it applies equally to agencies and organisations, subject to appropriate exceptions. One option is to limit assignment in the first place, following the precedent in HRIPA, whereby an agency may only assign identifiers if the assignment is *reasonably necessary to enable the agency to carry out any of its functions efficiently*. Further, the exceptions available to organisations regarding use and disclosure could also be made available to agencies.

10.20 On balance, however, in its final report, the ALRC's preference was to exclude agencies from coverage except on a case-by-case basis. It concluded that "applying the identifier principle to agencies could seriously impede activities for a public benefit, including: programs designed to reduce fraud and identity theft, service delivery and research".²¹ The ALRC suggested that, rather than adopting an identifier principle that would be "subject to several agency specific restrictions", it would be preferable "to regulate the assignment, collection, adoption, use and disclosure of identifiers by agencies on a case by case basis by means of separate legislation or guidelines".²² UPP 10 is therefore applicable to organisations only but can be extended to agencies on a case-by-case basis.

The proposed identifier principle

10.21 Having reviewed NPP 7 in the light of the submissions received, the ALRC recommended that the UPPs should contain a principle called

18 ALRC IP 31 Question 4-28.

19 ALRC DP 72 Proposal 27-1.

20 ALRC Report 108 vol 2 [30.26].

21 ALRC Report 108 vol 2 [30.34].

22 ALRC Report 108 vol 2 [30.36] – [30.37].

'Identifiers' that applies to organisations.²³ The proposed identifier principle, UPP 10 provides as follows:

UPP 10. Identifiers (only applicable to organisations)

10.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

- (a) an agency;
- (b) an agent of an agency acting in its capacity as agent;
- (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or
- (d) an Australian state or territory agency.

10.2 Where an identifier has been 'assigned' within the meaning of UPP 10.1 an organisation must not use or disclose the identifier unless:

- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency that assigned the identifier;
- (b) one or more of UPP 5.1(c) to (f) apply to the use or disclosure; or
- (c) the identifier is genetic information and the use or disclosure would be permitted by the new *Privacy (Health Information) Regulations*.

10.3 UPP 10.1 and 10.2 do not apply to the adoption, use or disclosure by a prescribed organisation of a prescribed identifier in prescribed circumstances, set out in regulations made after the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned.

10.4 The term 'identifier', for the purposes of UPP 10, includes a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:

- (a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or
- (b) is determined to be an identifier by the Privacy Commissioner.

23. ALRC Report 108 Recommendation 30-1.

However, an individual's name or ABN, as defined in the *A New Tax System (Australian Business Number) Act 1999* (Cth), is not an 'identifier'.

Note: A determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act 2003* (Cth).

Ambit and distinguishing features of UPP 10

10.22 In addition to considering the need for an identifier principle and its application to agencies, the ALRC also reviewed the current NPP 7 and considered the appropriateness of the definition of an identifier, the content of the principle, the issue of multi-purpose identifiers and the regulation of tax file numbers. The UPP was drafted so as to improve NPP 7 where necessary, based on issues raised and submissions received, and to this extent can be distinguished from NPP 7. It can also be distinguished from HPP 12. The distinguishing features are dealt with below.

Definition of "Identifier"

10.23 HRIPA's definition of an identifier is that it is usually, but not necessarily, a number, but never an individual's name.²⁴ NPP 7, on the other hand, does not describe what an identifier is; rather, it provides that it "includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations". Given its inclusive nature, it could cover a wide range of other identifiers with the specific exception of an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999* (Cth)).

10.24 In DP 72, the ALRC considered a range of issues regarding the definition of an identifier, including whether the definition should include identifiers that are not technically unique, those that contain biometric information and whether an individual's name and ABN should continue to be excluded.

Should identifiers be unique?

10.25 The current definitions of identifiers in NPP 7 and in HRIPA²⁵ require that identifiers be unique: "to identify *uniquely* the individual".

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

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

However, submissions to IP 31 pointed out that some identifiers, such as Medicare numbers, are not in fact unique.²⁶ For instance, a child may be listed on both parents' separate Medicare cards.

10.26 There is also the additional problem of matching a biometric sample with a stored template. The ALRC used the example of a collected sample, such as a facial image, being affected by lighting conditions, camera distance and lens precision, and therefore distorting the accuracy of the match.²⁷

10.27 The ALRC's suggested response in DP 72 was that the Privacy Commissioner be empowered to make a determination that, even where an identifier as defined does not of itself uniquely identify an individual, it would still be considered an "identifier" for the purposes of the principle. Various submissions took issue with this suggestion but the ALRC maintained that a determination-making power of the kind proposed in DP 72 would allow the Privacy Commissioner to determine that identifiers that are not actually unique would still be considered identifiers for the purposes of the identifier principle.²⁸ Thus, UPP 10 continues to require that identifiers be unique with the possibility of being determined as an identifier by the Privacy Commissioner.

Should biometric information be specifically included?

10.28 Biometric information has been described as information that relates to the physiological or behavioural characteristics of a person²⁹ and can be used as an identifier, such as agencies' use of an Australian ePassport for identification purposes. Given the risks associated with handling such information, the ALRC recommended that the definition of sensitive information be amended to include biometric information collected for certain purposes.³⁰

10.29 Neither the definition of an identifier in NPP 7 nor in HRIPA make specific reference to biometric information, although, being inclusive definitions, they are probably framed in broad enough terms to cover

26. ALRC DP 72 vol 2 [27.37].

27. ALRC Report 108 vol 2 [30.42].

28. ALRC Report 108 vol 2 [30.46].

29. ALRC Report 108 vol 2 [30.48], citing Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 4.

30. ALRC Report 108 vol 1 Recommendation 6-4. For "sensitive information" see para 2.88-2.147.

non-numerical information such as biometric information. However, having reviewed the submissions, the ALRC was of the view that the definition of an identifier should reflect the concerns about biometric information. Accordingly, it was proposed in DP 72 that the definition should include “a number, symbol or any other particular”.³¹ While many submissions supported this proposal, there was also a view that the definition of an identifier should go further and make an “overt reference” to biometric information.³²

10.30 Having weighed up the submissions, including those that expressed concerns about broadening the definition,³³ the ALRC recommended that UPP 10 should specifically refer to biometric information within the definition. Given that specific inclusion of biometric information merely makes it explicit, the criticisms levelled against such inclusion would appear to be irrelevant. While the definition is still inclusive, making wider coverage of other non-numerical information possible, it is noteworthy that the definition in UPP 10 no longer has the broad catch-all category of “any other particular” as was previously proposed in DP 72. However, the Privacy Commissioner’s power of determination under UPP 10.4(b), which allows the Privacy Commissioner to further broaden the scope of the definition, can be used

31. ALRC DP 72 Proposal 27-2. A number of stakeholders supported this proposal: Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007; Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

32. Privacy NSW, *Submission PR 468*, 14 December 2007.

33. The Attorney-General’s Department, in its submission to the ALRC, made reference to two concerns:

- (a) that inclusion in the definition of sensitive information of certain types of biometric information could result in an anomalous situation where collection of such information with consent would be permitted under UPP 2.6 but not used or disclosed as an identifier with consent under UPP 10.4;
- (b) biometric identifiers generated when a person enrolls in a biometric system are not unique to the agency or organisation and so can be independently generated by a number of agencies making proscription of adoption, use or disclosure of an identifier assigned by one agency unworkable: Australian Government Attorney-General’s Department, *Submission PR 546*, 24 December 2007.

in this regard. While biometric characteristics are generally considered to be unique to an individual, there are factors that may adversely affect this assumed uniqueness.³⁴ However, as noted above, the determination-making power is likely to cover such circumstances.

10.31 Another clarification that UPP 10 makes is that identifiers assigned by an agency to “verify” identity will also be covered under the definition of an identifier,³⁵ a matter of particular relevance in the context of biometric identifiers that are often used for identity verification.

10.32 It has been suggested, and the Commission agrees, that there is no justification for limiting the definition to collection of biometric information for the purpose of “*automated biometric* identification or verification ...” rather than any identification or verification that uses the identifier.³⁶ We believe that including any “other particular” in the definition as proposed in DP 72 and removing the limitation of collection to “automated biometric” identification would provide a broader definition.³⁷ However, the Commission is satisfied that any potential difficulties arising out of a restrictive definition may be alleviated by the Privacy Commissioner’s power of determination under UPP 10.4(b), referred to above. As such, in the interests of uniformity, the Commission supports the ALRC wording of the current definition as proposed in UPP 10.4.

Name and ABN number

10.33 As was the case with NPP 7, UPP 10 continues to exclude the individual’s name and ABN from the definition of “identifier”. While there appears no doubt that an individual’s name should be excluded since it is not information that is “assigned” to the individual, there may be some doubt about excluding an ABN number. Again, the Cyberspace Law and Policy Centre was firmly of the view that they saw no justification for excluding an ABN from this principle, particularly since

34. ALRC Report 108 vol 2 [30.42]-[30.43].

35. ALRC Report 108 vol 2 [30.58] Recommendation 30-3.

36. Cyberspace Law & Policy Centre UNSW, *Submission PR 487*, 19 December 2007, cited in ALRC Report 108 vol 2 [30.54].

37. Such a definition would read as follows:

The term ‘identifier’ for the purposes of UPP 10, includes a number, symbol, biometric information *or other particular* that is collected for the purpose of *identification* or verification that: [changes in italics].

“its legitimate use is accommodated by the Principle in the same way as for [TFNs]”.³⁸

10.34 In this regard, the ALRC was also of the view that the “exclusion of an ABN from the definition of ‘identifier’ may be a problem if there is a tendency among organisations or agencies to use the ABN of a sole trader to identify an individual acting in a non business capacity”. However, given that this issue was not raised in submissions, UPP 10 excludes the name and ABN from the definition.

Content of UPP 10

10.35 The identifier principle is set out in UPP 10.1 and states that an organisation must not adopt as its own identifier, an identifier that has been assigned by an agency, an agent of an agency, a contracted service provider for a Commonwealth contract or an Australian State or Territory agency.

10.36 UPP 10.2 states that, where an identifier has been so assigned, an organisation must not use or disclose the identifier unless the use or disclosure is necessary to fulfil its obligations to the agency, the exceptions listed in UPP 5.1(c)-(f) also apply, or the identifier is genetic information, the use or disclosure of which is allowed by the *Privacy (Health Information) Regulations*.

Exceptions

10.37 The exceptions to the prohibition on using and disclosing identifiers listed in UPP 10.2 and 10.3 are virtually identical to those listed in NPP 7.1A and 7.2. However, UPP 10.2(b) is subject to the exception in UPP 5.1(c)(i), which covers circumstances involving a serious threat to an individual’s life, health or safety, whereas NPP 7.2 is subject to NPP 2.1(e)(i), which covers circumstances involving a serious *and imminent threat*.³⁹ Also, NPP 7 and UPP 10 appear to differ in relation to genetic information but the effect of each is the same. NPP 2.1(ea) allows use or disclosure of genetic information, without consent, where it has been obtained in the course of providing a health service to an individual, and the use or disclosure is to prevent or lessen a serious threat to the life, health or safety of a genetic relative of the individual, it is disclosed to that genetic relative, and it is done in accordance with guidelines. By

38. Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007.

39. See para 5.27-5.30 for a discussion about the rationale behind this change.

contrast, UPP 10.2(c) simply allows use or disclosure of an identifier that is genetic information where this is permitted by the new *Privacy (Health Information) Regulations*, envisaged to include provisions similar to NPP 2.1(ea).⁴⁰

Circumstances of assignment and adoption

10.38 By contrast, UPP 10 and HPP 12 do vary in the circumstances in which assignment and adoption are permitted. Assignment is the process by which an agency selects a particular identifier to apply to an individual. HPP 12(1) provides that an organisation may only assign identifiers to individuals if the assignment *is reasonably necessary to enable the organisation to carry out any of its functions efficiently*.⁴¹ While this condition has been discussed above in the context of its potential to extend the identifier principle to agencies, while still imposing an inbuilt limitation,⁴² it is omitted in UPP 10. UPP 10 is solely focused on ensuring “single use” of identifiers by providing that an organisation must not adopt as its own an identifier that has been assigned by another agency.

10.39 The benefit of regulating the assignment of identifiers is that it would encourage good privacy practice as organisations would consider the necessity of assigning an identifier. The ALRC in DP 72 raised the issue of whether the assignment of identifiers should also be regulated by the identifier principle. The majority of submissions opposed regulating assignment on the basis that it would create unnecessary complexity, given that agencies and organisations frequently assign identifiers solely for internal use.⁴³ However, as pointed out by the ALRC, assignment could become an issue of concern where the identifier might be adopted, used or disclosed by another agency.⁴⁴

40. ALRC Report 108 Recommendation 63-5.

41. See also *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 7.1 (applicable to public and private sector organisations); *Information Act 2002* (NT) sch, IPP 7.1 (applicable to public sector organisations); *Information Privacy Act 2000* (Vic) sch 1, IPP 7.1.

42. See para 10.19.

43. Medicare Australia, *Submission PR 534*, 21 December 2007; Australian Government Department of Human Resources, *Submission PR 541*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007, cited in ALRC Report 108 vol 2 [30.84].

44. ALRC Report 108 vol 2 [30.86].

10.40 Another related issue is that UPP 10 does not regulate the adoption, use and disclosure by organisations of identifiers assigned by other organisations. Although no evidence was presented on the harm that could result from the use and disclosure of identifiers assigned by organisations, the ALRC did note that such use or disclosure may facilitate data matching activities undertaken by organisations.

10.41 The ALRC's view is that the greater risks are associated with adoption rather than assignment, and that agencies and organisations frequently assign identifiers for internal use. Though not regulated, the ALRC agrees with the Office of the Federal Privacy Commissioner ("OPC") that agencies should consider the necessity for assignment of an identifier, particularly when that identifier may be adopted, used or disclosed by another agency.⁴⁵ This is consistent with HPP 12 in relation to assignment by agencies and private sector persons.

Consent

10.42 Consent to use and disclose identifiers is another notable area of variance. HPP 12(2) allows a private sector person to adopt as their own identifier one that has been assigned by an agency where the individual consents. Similarly, HPP 12(3) allows a private sector person to use or disclose an identifier assigned by an agency where the individual consents. Some States and Territories also provide for a consent exception.⁴⁶ However, neither NPP 7 nor UPP 10 provide for consent of an individual as an exception to the use, disclosure or adoption of identifiers.

10.43 In considering whether consent ought to be an exception, some organisations, such as Centrelink, submitted to the ALRC that this restriction (of not having consent) applicable to the identifier principle "impedes the operation of a number of its existing services, which provide information to organisations about the concessional status of the individual with the consent of the individual concerned".⁴⁷ Arguably, allowing individuals to consent would allow organisations greater efficiency in the delivery of services.

45. The concerns of multi-purpose identifiers are addressed at para 10.57.

46. *Information Privacy Act 2000* (Vic) sch 1, IPPs 7.2(b), 7.3(c); *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 7(2)(b); *Information Act 2002* (NT) sch, IPPs 7.2(b), 7.3(b).

47. ALRC Report 108 vol 2 [30.89].

10.44 On the other hand, the OPC was of the view that allowing use and disclosure where it has been consented to can lead to problems because “individuals may not always be conscious of the inherent risks of consenting to incrementally greater uses of their unique identifier”.⁴⁸ The ALRC agreed with the OPC that the privacy risks associated with an individual being able to consent to the use or disclosure or adoption of an identifier would give rise to privacy risks. Further, the ALRC was of the view that a general consent exception would significantly reduce the protection afforded by the identifier principle.⁴⁹

10.45 In CP 3, the Commission raised the issue of whether the privacy principle regulating the use and disclosure of identifiers should be in the same terms as HPP 12 or the proposed UPP 10 or a combination of the two.⁵⁰ Commenting on this issue, the Australian Privacy Foundation and the Cyberspace Law & Policy Centre observed that HPP 12 has too many exceptions that undermine its effect.⁵¹ The Inner City Legal Centre was of the view that UPP 10 gives greater protection around identifiers by ensuring single use and restricting disclosure.⁵²

10.46 Rather than provide for a general consent exception, UPP 10.3 makes provision for exceptional circumstances to be accommodated by way of regulations similar to existing regulations that allow an individual to consent to the disclosure of his or her Centrelink Customer Reference Number.⁵³

10.47 The disadvantage of allowing exceptions via regulations is that the process of making regulations is resource intensive.⁵⁴ However, provided procedural safeguards are included, exceptions introduced via regulations should ensure that the consent given does not give rise to avoidable privacy concerns that an individual giving consent may not necessarily fully appreciate.

48. Office of the Federal Privacy Commissioner, *Submission PR 499*, 20 December 2007, cited in ALRC Report 108 vol 2 [30.90].

49. ALRC Report 108 vol 2 [30.92].

50. NSWLRC CP 3 Issue 44.

51. Australian Privacy Foundation, *Submission* and Cyberspace Law and Policy Centre UNSW, *Submission*.

52. Inner City Legal Centre, *Submission*.

53. ALRC Report 108 vol 2 [30.92]-[30.93].

54. ALRC Report 108 vol 2 [30.89].

10.48 There is, however, an exception allowing consent to the general prohibition against an organisation collecting sensitive information about an individual. The definition of sensitive information includes biometric information. Thus, while a person may consent to an organisation collecting biometric information about him or her, an individual cannot consent to enable an organisation to use or disclose biometric information as an identifier. Although the Attorney-General's Department viewed this as an anomaly and a cause for arguing against including biometric information within the definition of an identifier,⁵⁵ the ALRC did not appear to be swayed by this concern. In the Commission's view, there is a distinct difference in the privacy risks associated with consenting to the collection of biometric information and consenting to the use and disclosure of the same as an identifier, the risks in the latter case being much greater.

Practical application of UPP 10

10.49 While identifiers are critical in the process of identification, the practical application of UPP 10 is determined by what falls within and outside that process. If the process does not use an identifier or is not meant for identification purposes, then UPP 10 will not apply.

Verification through sighting

10.50 Identity verification is the process of confirming through documentary or other evidence that a person is who they claim to be and this is usually done by sighting an identifier. Thus, a person purchasing cigarettes or alcohol may be required to show a document to prove his or her age. Such a practice is not intended to be regulated by the identifier principle by preventing an organisation from use or disclosure for the purpose of verifying an individual's identity. Such use or disclosure will not permit secondary use for the purposes of data matching.⁵⁶ If the identifier principle did inhibit verification, it was suggested that the Privacy Commissioner develop guidance to address the issue.⁵⁷

55. Australian Government Attorney-General's Department, *Submission PR 546*, 24 December 2007, cited in ALRC Report 108, vol 2 [30.52].

56. ALRC Report 108 vol 2 [30.71].

57. ALRC Report 108 vol 2 [30.72].

Data matching

10.51 Data matching has been described as “the large scale comparison of records or files ... collected or held for different purposes, with a view to identifying matters of interest”.⁵⁸

10.52 Data matching is currently regulated by the Privacy Commissioner’s monitoring and research functions, the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and the Data-matching Program (Assistance and Tax) Guidelines and other Guidelines, as well as NPP 2 and Principle 11, which regulate the disclosure of information by an agency or organisation for the purposes of data matching.

10.53 The identifier principle itself also provides some regulation of data matching in that an organisation is prohibited from adopting an identifier unless it is for a specified purpose. However, data matching is not always done by means of identifiers. It is possible that data sets may be linked by the use of names or dates of birth⁵⁹ that do not fall within the definition of an identifier.

10.54 Although there was concern about the inadequate regulation of data matching, the ALRC is of the view that data matching is not inherently linked to identifiers and should not be regulated by the identifier principle. Rather, the ALRC recommended that data matching activities should be regulated separately to the identifier principle through guidelines on the privacy implications of data matching to be developed and published by the OPC.⁶⁰

Application to State and Territory agencies

10.55 NPP 7.1 does not apply to identifiers issued by State and Territory agencies; it is limited in application to preventing organisations from adopting an identifier that has been assigned by “an Australian Government agency, an agent of that agency or a contracted service provider of an Australian Government agency”.

10.56 This limitation means that identifiers such as driver’s licences issued by State and Territory agencies will not fall within the current definition. The ALRC in Report 108, noted that stakeholders were

58. ALRC DP 72 vol 2 [27.46].

59. Office of Victorian Privacy Commissioner, *Submission PR 217*, 28 February 2007, cited in ALRC Report 108 vol 2 [30.74].

60. ALRC Report 108 vol 2 [30.76].

generally supportive of extending coverage to State and Territory agencies. Accordingly, UPP 10 extends coverage to regulate the adoption, use and disclosure by organisations of identifiers assigned by State and Territory agencies. However, such extension is only intended to cover the situation where an identifier is collected for inclusion in a record, rather than merely for sighting or verification purposes.

Multi-purpose identifiers

10.57 Multi-purpose identifiers are unique identifiers assigned to individuals for use by multiple agencies and organisations. Such use has the important benefit of increasing administrative efficiency. However, it also gives rise to many privacy concerns by extending the government's power over, and access to, an individual's personal information including information pertaining to financial, health and family status. Such use also greatly facilitates the data matching process when the available information is combined, further eroding an individual's privacy.⁶¹

10.58 The ALRC considered the issue of multi-purpose identifiers against the background of the history of identification schemes, particularly in the context of the proposed access card, which would have replaced many health care and social services cards. It concluded that 'multi-purpose identifiers pose significant privacy risks'.⁶²

10.59 Many submissions were supportive of the ALRC's proposal in DP 72 that the Australian Government should, in consultation with the Privacy Commissioner, consider the need for a privacy impact assessment before introducing a multi-purpose identifier. Some stakeholders supported mandatory impact statements in view of the significant privacy risks involved with the use of multi-purpose identifiers.⁶³ Others have raised the issue of the potential for impact statements to be not completely impartial, and have suggested that an independent and public privacy assessment should be commissioned by the government before introducing a multi-purpose identifier. The ALRC has recommended that the Australian Government should conduct a

61. ALRC DP 72 vol 2 [27.77]-[27.83].

62. ALRC Report 108 vol 2 [30.128].

63. ALRC Report 108 vol 2 [30.126].

privacy impact statement before the introduction of any multi-purpose identifier.⁶⁴

THE COMMISSION'S VIEW

10.60 Overall, the Commission supports the inclusion of a separate privacy principle to regulate identifiers. As to the ALRC's decision to exclude agencies from general coverage, while we believe the rationale for regulating identifiers is just as capable of application to agencies as to organisations, we agree with the ALRC's justification that it could seriously impede activities for a public benefit. For this reason, we support the exclusion of agencies and agree with extension on a case by case basis either in separate sectoral legislation or by means of guidance provided by the Privacy Commissioner.

10.61 In terms of the content and application of UPP 10, the Commission supports all other recommendations that have shaped UPP 10 as it currently stands, with the exception of the exclusion of ABNs from the definition of identifiers. The Commission can see no reason why ABNs should be treated any differently from TFNs and recommends that the exclusion be removed.

RECOMMENDATION 12

UPP 10.4 should be amended so as to remove the exclusion of ABNs from the definition of identifiers.

64. ALRC Report 108 Recommendation 30-6.

11.

UPP 11: Cross-border data flows

- Introduction
- Current approaches to regulation of cross-border data flows
- ALRC Report 108
- Content and distinguishing features of UPP 11
- Defining accountability
- The scope of application of UPP 11
- Adequacy of remedial action
- Interaction with other UPPs
- The Commission's overall views

INTRODUCTION

11.1 Cross-border data flows, sometimes referred to as cross-border data transfers or transborder data flows, is about the movement of personal information across national borders or State borders, as the case may be.

11.2 With the communication revolution taking over and the current trend of outsourcing back office services resulting in the globalisation of modern business more than ever before, personal information is now transferred across State borders and further afield between nations, with incredible ease. In addition, the current economic climate of globalisation of information and electronic commerce demand such cross-border data flows to ensure economic growth.

11.3 However, the unregulated or under regulated transfer of personal information can result in a widespread intrusion of privacy for affected individuals, whether they be consumers or citizens, thereby undermining or weakening all other privacy protection. Indeed, the *Community Attitudes to Privacy 2007* survey conducted by the Office of the Federal Privacy Commissioner (“OPC”) revealed that “the majority of Australians (90%) are *concerned* about businesses sending their personal information overseas, with 63% being *very concerned*”.¹ Similar concerns were expressed in the National Privacy Phone-In conducted by the ALRC in June 2006 as well as in submissions to the ALRC.²

11.4 Individuals need to be confident that their personal information is protected by the agency or organisation that has access to, or control of, such information and that they have avenues of redress, if their privacy is breached. While the protection of privacy must not be compromised, there should also be a free flow of information without the creation of unnecessary obstacles and barriers. It is therefore imperative that the regulation of cross-border data flows by various international

-
1. Wallis Consulting Group, *Community Attitudes Towards Privacy 2007* (2007), 36, Office of the Privacy Commissioner website «www.privacy.gov.au/materials/types/download/8820/6616» at 10 August 2009.
 2. National Privacy Phone-In June 2006. See also Unisys, *Submission PR 569*, 12 February 2008; B Laing, *Submission PR 339*, 12 November 2007, cited in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) (“ALRC Report 108”) vol 2 [31.4]-[31.5].

frameworks and federal and State legislation be appropriate and adequate to ensure a healthy balance is struck between cross-border flow of information and the protection of privacy.

11.5 The aim of this chapter is to ascertain if this balance has been appropriately struck in UPP 11. In making this evaluation, the Commission examines the content and likely impact of UPP 11 against the background of existing approaches adopted in international frameworks and Commonwealth and NSW legislation, to assess the effectiveness of the principle and its suitability for adoption in NSW.

CURRENT APPROACHES TO REGULATION OF CROSS-BORDER DATA FLOWS

11.6 Internationally, cross-border data flow is regulated by various frameworks. Of particular relevance are the European Union Data Protection Directive (“EU Directive”)³ and the Asia-Pacific Economic Cooperation (“APEC”) Privacy Framework. The Asia-Pacific Privacy Charter (“the Charter”), a regional non-government expert group, is also developing independent privacy standards for use in the region.

11.7 The frameworks adopted internationally have resulted in the emergence of two approaches to the regulation of cross-border data transfers. They are:

- the “adequacy” approach taken by the EU Directive; and
- the “accountability” approach taken by APEC.

11.8 These two approaches have been adopted to a greater or lesser extent either in combination or singly by privacy legislation in Australia and overseas.

The adequacy approach

11.9 Article 25(1) of the EU Directive prohibits the transfer of personal data to any country or territory outside the EU (a third country) unless the third country “ensures an *adequate* level of protection” (emphasis added) for the rights and freedoms of those individuals whose personal data is being transferred, hence referred to as the adequacy approach.

3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/95, 31-50.

11.10 Where there is inadequate protection, the transfer of personal data can still be legitimised if, as provided in Article 26:

- there is unambiguous consent from the data subject;
- the transfer is necessary for the performance, implementation or conclusion of certain contractual transactions;
- the transfer is in the public interest or the vital interests of the data subject; or
- the transfer is made from a public register.

11.11 The most notable characteristic of this approach is that it establishes comprehensive privacy regulation that covers both the public and private sectors. The general approach is to allow the transfer of data to countries only if they provide adequate protection⁴ or if the transfer falls within an exceptional circumstance.

11.12 Article 25(2) sets out the criteria against which adequate protection is assessed as follows:

The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

11.13 The Data Protection Working Party of the European Commission, comprising representatives of supervisory authorities in EU member states, a representative of the authority or authorities established for the Community institutions and bodies and a representative of the European Commission, makes the decision about the adequacy of the protection afforded by a third country.⁵ However, there appears to be some

4. Countries that have been assessed as 'adequate' for this purpose are: Canada, Switzerland, Argentina, Guernsey and the Isle of Man. The US Department of Commerce's Safe Harbour Privacy Principles and the 'transfer of Air Passenger Name Records to the United States Bureau of Customs and Border protection' have also been given adequacy status: ALRC Report 108 vol 2 [31.17]. Australian privacy law has not yet gained formal recognition by the EU as being adequate: ALRC Report 108 vol 2 [31.21] - [31.28].

5. EU Directive, Article 29 and ALRC Report 108 vol 2 [31.17].

uncertainty as to who exactly should make the assessment decision: “the data controller, the supervisory authority or some other body established by Member State procedure”.⁶

11.14 The European Commission is also of the view that there are wide divergences in implementation.⁷ The strong emphasis in the EU Directive on registration requirements such as notification⁸ and publication⁹ have been considered to be “burdensome and expensive”¹⁰ and not required for the EU test of adequacy.

11.15 Most importantly, the EU Directive does not cover law enforcement and security activities in an integrated way, resulting in a trend towards far-reaching exemptions for law enforcement purposes without detailed justification.¹¹ It has been suggested that providing the consumer with a number of accountability bodies to which they can complain makes it hard for the consumer and the regulator.¹²

The accountability approach

11.16 The APEC Privacy Framework was published in 2004 and is “principles based” with nine privacy principles largely based on the 1980 Organisation for Economic Co-operation and Development (“OECD”) Guidelines on the Protection of Privacy and the Transborder Flow of Personal Data. One of the APEC principles applies specifically to the

-
6. European Commission, Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Working Document, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP 12)*, Adopted by the Working Party 24 July 1998, 26.
 7. Commission of the European Communities, *Report from the Commission: First Report on the implementation of the data protection Directive (2003) 95/46/EC*, 19.
 8. EU Directive, Articles 18 and 19.
 9. EU Directive, Article 21.
 10. G Sutton, Z Xinbao and T Hart, *Personal Data Protection in Europe and China: What lessons to be learned?* EU-China Information Society Project, November 2007, China Information Society News «http://www.information-society.de/files/DP_EU-China2007.pdf» at 14 September 2009.
 11. C Connolly, *Asia-Pacific Region at the Privacy Crossroads* (2008), 3. The EU approach, Galexia Pty Ltd «http://www.galexia.com/public/research/articles/research_articles-pa06.html» at 10 August 2009.
 12. *Meeting Privacy Challenges: ALRC and NSWLRC Privacy Reviews Seminar*, Panel Session 4, Faculty of Law, UNSW, Sydney, 2 October 2008.

issue of accountability in the transfer of information whether domestically or internationally and provides as follows:

A personal information controller should be accountable for complying with measures that give effect to the principles stated above. When personal information is to be transferred to another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these principles.

11.17 As an alternate approach to the EU Directive, the accountability approach involves greater reliance on self regulation, self certification, trust marks and the registration of corporate rules. Rather than focussing on border controls as does the adequacy approach, the accountability approach emphasises that “accountability should follow the data”.¹³ Properly applied, it has been argued that the accountability approach can address “country risk” very simply because the original collector of the information will be accountable for the transfer of the personal information, which will in turn offer a better chance of enforcement.¹⁴

11.18 On the other hand, it has been argued that the accountability approach is too “light touch” with a bias towards the free flow of information, rather than limiting the export of information to stringently crafted exceptional circumstances.¹⁵ Noticeably, there is no explicit limitation of data flows to countries that do not have similar privacy laws or protections.¹⁶

The Australian approach

Federal approach

11.19 Federally, cross-border data flow is regulated by privacy principles in the *Privacy Act 1988* (Cth), which applies to acts done, or practices engaged in, outside Australia by an organisation, if the acts or practices

13. ALRC Report 108 vol 2 [31.49].

14. *Meeting Privacy Challenges: ALRC and NSWLRC Privacy Reviews Seminar*, Panel Session 4, Faculty of Law, UNSW, Sydney, 2 October 2008.

15. See G Greenleaf, “APEC’s Privacy Framework: A New Low Standard” (2005) 11 *Privacy Law & Policy Reporter* 121, 122.

16. The lack of this principle in the APEC Privacy framework distinguishes it from the Asia-Pacific Privacy Charter which otherwise shares many similarities with the APEC Framework.

relate to personal information about an Australian citizen or permanent resident, and provided the organisation either:

- (a) is linked to Australia by being a citizen or a permanent resident, or an unincorporated association, trust, partnership or body corporate formed in Australia; or
- (b) carried on a business in Australia and held or collected information in Australia either before or at the time of the act done or practice engaged in.¹⁷

11.20 Section 5B further provides for extra-territorial operation by empowering the Privacy Commissioner to take action overseas to investigate and deal with complaints about overseas acts and practices. Notably though, it applies only to organisations and not to agencies. Section 13D provides that where an act or practice is required by the law of a foreign country, it will not be overridden by the Privacy Act.

11.21 The circumstances in which an organisation may transfer personal information is dealt with in NPP 9, set out below, which is largely modelled on the adequacy approach as spelled out in Articles 25 and 26 of the EU Directive. NPP 9 prohibits the transfer of personal information unless one of the conditions in (a)–(f) is satisfied.

NPP 9: Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

- (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or
- (b) the individual consents to the transfer; or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

17. *Privacy Act 1988* (Cth) section 5B, as paraphrased by the ALRC at ALRC Report 108 vol 2 [31.71].

- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
- (e) all of the following apply:
 - (i) the transfer is for the benefit of the individual;
 - (ii) it is impracticable to obtain the consent of the individual to that transfer;
 - (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
- (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

NSW approach

11.22 In NSW, s 19(2) of PPIPA prohibits disclosure of information outside NSW or to a Commonwealth agency unless:

- (a) a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction or applies to that Commonwealth agency; or
- (b) the disclosure is permitted under a privacy code of practice.

11.23 Section 19(4) indicates that the “Privacy Commissioner is to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales and to Commonwealth agencies” and s 19(5) states that 19(2) does not apply unless a code referred to in 19(4) is made. Given that no privacy codes of practice have, to date, been made, there are, in effect, currently no limitations on the disclosure of personal information outside NSW.¹⁸

11.24 However, HRIPA regulates disclosure of health information to Commonwealth agencies by virtue of HPP 14, subject to eight conditions.

18. This was the Commission’s view in CP 3 [6.61]-[6.62] consistent with the advice of the Crown Solicitor and the Privacy Commissioner. This view has been further confirmed in *GQ v NSW Department of Education and Training (No 2)* [2008] NSWADT 319.

HPP 14: Transborder data flows and data flow to Commonwealth agencies

An organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

- (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or
- (b) the individual consents to the transfer, or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request, or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or
- (e) all of the following apply:
 - (i) the transfer is for the benefit of the individual,
 - (ii) it is impracticable to obtain the consent of the individual to that transfer,
 - (iii) if it were practicable to obtain such consent, the individual would be likely to give it, or
- (f) the transfer is reasonably believed by the organisation to be necessary to lessen or prevent:
 - (i) a serious and imminent threat to the life, health or safety of the individual or another person, or
 - (ii) a serious threat to public health or public safety, or
- (g) the organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles, or
- (h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

ALRC REPORT 108

11.25 The issue of cross-border data flows was dealt with at length by the ALRC in DP 72 as well as in Report 108 with a view to improving the regulation of cross-border data flows currently contained in NPP 9. The result was the formulation of UPP 11, set out below, which adopts the new accountability approach while incorporating aspects of the existing adequacy approach.

UPP 11: Cross-border Data Flows

11.1 If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless the:

- (a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to these principles;
- (b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or
- (c) agency or organisation is required or authorised by or under law to transfer the personal information.

Note: Agencies and organisations are also subject to the requirements of the 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.

CONTENT AND DISTINGUISHING FEATURES OF UPP 11

11.26 The following section addresses the content of UPP 11 and its approach to regulating cross-border data flows, while distinguishing it from NPP 9 and HPP 14. It evaluates the rationale for change and assesses UPP 11's overall potential for effectiveness. It also makes recommendations for change, where appropriate.

Coverage

11.27 As stated above, the Privacy Act applies to acts done, or practices engaged in, outside Australia by an organisation, but does not extend to

agencies.¹⁹ The ALRC proposed in DP 72 and Report 108 that the Privacy Act be amended to clarify that agencies that operate outside Australia should be subject to the Privacy Act.²⁰ This represents a departure from HPP 14 which only applies to organisations, and s 19(2) of PPIPA which only applies to agencies and is currently inoperative.²¹

11.28 This lack of regulation of cross-border flows by agencies was discussed at length in the ALRC’s DP 72 and Report 108. There appears no rational justification for this exclusion and the majority of submissions supported extending coverage to agencies. Accordingly, UPP 11 applies to agencies and organisations. This is a significant improvement on the current provisions. The Commission supports it.

Terminology

11.29 Whereas NPP 9 referred to the transfer of personal information to “someone ... who is in a foreign country”, UPP 11 refers to a “recipient ... who is outside Australia and an external territory”. The ALRC’s rationale for this change in terminology is that it clarifies that “the principle applies to the overseas transfer of personal information to agencies, organisations and individuals” and that it suggests “a broader reading of what an overseas jurisdiction may be” consistent with the language used in other cross-border regulatory principles. This is also why the principle is now referred to as “Cross-border data flows” rather than “Transborder data flows”.²²

“Transfer”

11.30 The ALRC Report considered whether the term “transfer” ought to be defined to distinguish it from “use” and “disclosure”, and generally to clarify what a “transfer” of personal information would include. Of particular concern was whether the focus ought to be on the *opportunity* to access the information or *actual* access.

11.31 The OPC submitted that the term “transfer” should be defined but “should not exclude information transferred overseas accidentally because the sending entity has not taken reasonable steps to protect the

19. *Privacy Act 1988*(Cth) s 5B.

20. ALRC Report 108 vol 2 [31.79].

21. See para 11.22-11.24.

22. ALRC Report 108 vol 2 [31.175].

personal information”.²³ Microsoft, on the other hand, submitted that emerging technologies make it hard to formulate a definition.²⁴ Overall, there was a lack of consensus on the ambit of a definition.²⁵

11.32 The ALRC’s view was that the ambit of “transfer” was unclear and, therefore, the principle really turned on whether the personal information was accessed or not. If accessed it would be subject to the principle.²⁶ Ultimately however, the ALRC preferred to rely on OPC guidance rather than on legislative definition to accommodate the potentially frequent changes and consequent amendments that would be required as a result of the rapid advances in technology.²⁷

11.33 Another relevant issue in the context of transfers is whether the cross-border principles should apply equally to transfers by an organisation to another part of the same organisation overseas and another related company. Currently, transfers to another part of the same organisation are not prevented by NPP 9 but transfers to a related company must comply with NPP 9. However, s 13B(1) of the Privacy Act states that “the disclosure of personal information (other than sensitive information) about the individual by the body corporate to a related body corporate” is not an interference with privacy. While there may be justification for related bodies corporate to transfer information between each other, there is an apparent discrepancy between s 13B and NPP 9. Despite a few submissions that argued to the contrary,²⁸ the ALRC recommended that s 13B be amended to make it consistent with the approach adopted in NPP 9 and followed in UPP 11: that if an organisation transfers personal information to a related body corporate outside Australia or an external territory, the transfer will be subject to the Cross-border Data Flows principle.²⁹

23. Office of the Privacy Commissioner, *Submission PR 499*, 20 December 2007, quoted at ALRC Report 108 vol 2 [31.186].

24. Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007, quoted in ALRC Report 108 vol 2 [31.187].

25. ALRC Report 108 vol 2 [31.182]- [31.191].

26. ALRC Report 108 vol 2 [31.192].

27. ALRC Report 108 vol 2 [31.194].

28. Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007; GE Money Australia, *Submission PR 537*, 21 December 2007, referred to in ALRC Report 108 vol 2 [31.201]-[31.202].

29. ALRC Report 108 vol 2 Recommendation 31.5.

Approach

11.34 The most notable difference between NPP 9 and UPP 11 is the shift in approach from a focus on adequacy to one of accountability. Rather than prevent the transfer of information unless particular conditions are met, as is the case with NPP 9, in UPP 11 the default is based on the accountability concept, whereby transfers are allowed if there is accountability. The adequacy (of laws, contracts and binding schemes) concept is presented as an exception to the accountability approach.

11.35 In DP 72, the ALRC linked the accountability approach to a number of conditions that are found in NPP 9, particularly clauses (c) to (f), with some modifications.³⁰ Many stakeholders³¹ submitted that this would be a positive step towards ensuring that agencies and organisations are responsible about how they transfer personal information, enabling the consumers to identify the agency or organisation when breaches occur.³²

11.36 However, this approach also met with significant opposition on the basis that the protection afforded by NPP 9 was sufficient and because of operational concerns.³³ Some submissions objected to the conditions of transfer and were of the view that “the APEC notion of accountability alone is sufficient to regulate transborder data flows”.³⁴ Others objected to the limited scope for a transferor to provide a defence to liability³⁵ and argued that it should be “sufficient that an organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the proposed UPPs”.³⁶

30. ALRC DP 72 Proposal 28-4.

31. ALRC Report 108 vol 2 [31.107]-[31.108].

32. See C Connolly, “Weak protection for offshore data – the ALRC recommendations for Cross-border Transfers” (2008) 5 (3-4) *Privacy Law Bulletin* 42, 43.

33. ALRC Report 108 vol 2 [31.109]-[31.118].

34. Microsoft Asia Pacific, *Submission PR 463*, 12 December 2007, quoted in ALRC Report 108 vol 2 [31.114].

35. Australian Bankers’ Association Inc, *Submission PR 567*, 11 February 2008, cited in ALRC Report 108 vol 2 [31.111].

36. GE Money Australia *Submission PR 537*, 21 December 2007, quoted in ALRC Report 108 vol 2 [31.112].

11.37 Having considered the submissions, the ALRC decided to strip away the conditions proposed in the DP and to introduce a general accountability principle in UPP 11 as a default position. Thus, UPP 11 does not prevent information from being transferred, but requires that agencies and organisations remain accountable. They will be responsible under the Privacy Act for the acts and practices of a recipient of personal information, the subject of a cross-border transfer and will be subject to the complaints and investigation mechanisms of Part V of the Privacy Act.

11.38 The Commission considers the shift from the adequacy approach to the accountability approach a significant and workable development. However, its true effectiveness will depend on:

- the definition of “accountability”;
- the scope of application; and
- the adequacy of remedial action.

DEFINING ACCOUNTABILITY

11.39 In Report 108, the ALRC discussed how the accountability approach should operate as a default position in relation to cross-border transfers. It explained that the benefit of the approach is that while it does not prevent information from being transferred, it will require agencies and organisations to remain accountable for the information when transferred (except in the exceptional circumstances listed).³⁷

11.40 The ALRC also explained what accountability means in this context:

The general principle of accountability should mean that an agency or organisation will be responsible under the Privacy Act for the acts and practices of a recipient of personal information the subject of a cross-border transfer. That is, where an agency or organisation transfers information to a recipient outside Australia, if the acts or practices of that recipient in respect of the personal information would have amounted to an interference with the privacy of an individual if done in Australia, they should constitute an interference with the privacy of the individual for the purposes of the Privacy Act. Further, the acts or practices of the recipient should

37. ALRC Report 108 [31.119]-[31.126].

be taken to be acts or practices of the relevant agency or organisation for the purposes of the Privacy Act.³⁸

11.41 However, UPP 11 itself provides no definition of “accountability”. Commenting on UPP 11, the Cyberspace Law and Policy Centre was of the view that “a definition of ‘accountability’ must be added – accountability is meaningless in the current proposals”.³⁹ The Cyberspace Law and Policy Centre also suggested that:

The evidentiary burden should shift to the party that exports the personal information to a country that has no data protection laws equivalent to Australian laws. It should be up to them to prove, on the balance of probabilities, that any damage suffered by the person which might reasonably be assumed to be as a result of the breach of the UPPs by some overseas party has in fact arisen from some other cause.⁴⁰

11.42 This is consistent with the ALRC’s view on what accountability should mean.

11.43 The Commission agrees that, given the change of approach, a definition of “accountability” should be included. Identifying in clear terms what exactly is meant by “accountability” would also help to establish proof of whether UPP 11 has been breached. While the Commission supports the inclusion of a definition of “accountability” in the privacy principles, we do not believe that is appropriate to articulate the incidence of the burden of proof in high level principles of this nature.

38. ALRC Report 108 vol 2 [31.123].

39. 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), 38.

40. 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), 38.

RECOMMENDATION 13

An agency or organisation being “accountable” for personal information should be defined in UPP 11 to mean:

- (a) being responsible for the acts and practices of a recipient of personal information, the subject of a cross-border transfer; and
- (b) being liable for a breach of UPP 11 if the acts and practices of the recipient would have amounted to an interference with the privacy of an individual, if done in Australia.

THE SCOPE OF APPLICATION OF UPP 11

11.44 UPP 11.1 does not apply to all transfers of personal information as it is subject to three exceptions. The exceptions are listed in UPP 11.1(a) to (c). They can be paraphrased as follows:

- (a) the “reasonable belief” exception;
- (b) the “consent” exception; and
- (c) the “required or authorised by or under law” exception.

11.45 In contrast, NPP 9 is subject to six exceptions and HPP 14 is subject to eight. Though less in number, the question for consideration is whether the exceptions are still so wide that they render UPP 11 ineffective, or less effective than it should be.

Reasonable belief

11.46 UPP 11.1(a) provides for accountability of cross-border data flows unless the:

agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to these principles;

11.47 What precisely constitutes a “reasonable belief” or what constitutes a “substantially similar” set of principles is not explicit.

11.48 Commenting on the term “reasonable belief” in submissions to DP 72, many stakeholders observed that the test “is ambiguous”,⁴¹ and that “believing is not quite the same thing as knowing”,⁴² and expressed concern “about the practicality and reasonableness”⁴³ of the terms. It is possible that even a reasonable belief in error may invoke the exception, making it a very weak test. It has been suggested that such a test is “doomed to become a wide loop hole for transfers that weaken privacy, either through error or deliberate action”.⁴⁴

11.49 Similarly, the term “substantially similar to these principles” is undefined and no guidance has been offered on how such laws are to be identified. There may be instances where legislation in another jurisdiction is not “substantially similar” but provides adequate protection by taking an alternate approach and may even be more favourable.⁴⁵

11.50 It has also been observed that protection is restricted to being “substantially similar to ‘these principles’ [UPPs]”, being “a fraction of the potential breaches of privacy contained in the broader *Privacy Act*”.⁴⁶ This would exclude protections offered by the rest of the Privacy Act, such as data breach rules, as well as health and credit reporting regulations and other similar protections contained in the Act. As an example, it has been suggested that consumers are likely to be seriously concerned about a data breach, whether the breach occurs at a local data centre or an offshore data centre.⁴⁷ It would be preferable to cover all

41. Public Interest Advocacy Centre, *Submission PR 548*, 26 December 2007, cited in ALRC Report 108 vol 2 [31.131].

42. Confidential, *Submission PR 535*, 21 December 2007, quoted in ALRC Report 108 vol 2 [31.132].

43. Australian Communication and Media Authority, *Submission PR 522*, 21 December 2007, cited in ALRC Report 108 vol 2 [31.134].

44. C Connolly, “Weak protection for offshore data – the ALRC recommendations for Cross-border Transfers” (2008) 5 (3-4) *Privacy Law Bulletin* 42, 44.

45. 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), 36.

46. C Connolly, “Weak protection for offshore data – the ALRC recommendations for Cross-border Transfers” (2008) 5 (3-4) *Privacy Law Bulletin* 42, 44.

47. C Connolly, “Weak protection for offshore data – the ALRC recommendations for Cross-border Transfers” (2008) 5 (3-4) *Privacy Law Bulletin* 42, 44.

protection offered by the Privacy Act and regulations. This would apply to laws, binding schemes and contracts.

11.51 Despite objections in the submissions, and although the ALRC acknowledged the concerns raised, the ALRC did not recommend any changes to the reasonable belief test nor the test that protections must be substantially similar. Instead, it recommended that “the Australian Government should develop and publish a list of laws and binding schemes in force that effectively uphold principles for the fair handling of personal information that are substantially similar to the UPPs”⁴⁸ and that the OPC’s guidance on the Cross-border Data Flows principle should include guidance on what constitutes a reasonable belief.⁴⁹

11.52 The Commission agrees with the view expressed by Chris Connolly that if a list of countries that provides privacy protection substantially similar to the UPPs is published, then there would be no further need for the weaker reasonable belief test. On the other hand, if a country is not on the published list, the reasonable belief test can still be met, which creates a dangerous situation⁵⁰ because there will be no accountability and no protection in those circumstances. Either way, the reasonable belief test appears unnecessary and problematic, whether applied to laws, contracts or binding schemes.

Laws

11.53 The fact that a country has privacy laws does not necessarily mean that those privacy laws provide actual protection. For instance, Japan’s *Act on the Protection of Personal Information 2003* does not provide exhaustive coverage because many notable exceptions are not contained in the Act, but in other documentation such as Cabinet orders.⁵¹ There are many other examples of countries that do have privacy legislation, but

48. ALRC Report 108 Recommendation 31-6.

49. ALRC Report 108 Recommendation 31-7.

50. C Connolly, “Commentary on the ALRC Recommendations for Cross Border Transfers” (2008), 2, paper presented at *Meeting Privacy Challenges: ALRC and NSWLRC Privacy Reviews Seminar*, Faculty of Law, UNSW, Sydney, 2 October 2008, «http://www.cyberlawcentre.org/ipp/events/symposium08/materials/4_Connolly_Paper2.pdf» at 14 September 2009.

51. Cabinet Order for the enforcement of the Act on the Protection of Personal Information, 10 December 2003: referred to in C Connolly, “Weak protection for offshore data – the ALRC recommendations for Cross-border Transfers” (2008) 5 (3-4) *Privacy Law Bulletin* 42, 43.

which do not necessarily provide the requisite level of protection.⁵² A mistaken “reasonable belief” can therefore quite easily be maintained, even justified, at great risk to the person whose personal information has been transferred.

11.54 The ambiguities created by the presence of privacy legislation and the absence of evidence based, objective knowledge (rather than a belief) of the requisite level of protection suggests that it would be preferable to substitute the “reasonable belief” test with a test that requires actual protection. Such a test could be implemented by reference to an official list of jurisdictions that have adequate and effective privacy protections. Most submissions to the ALRC supported the development of such a list.⁵³ Its formulation would, no doubt, be a difficult and resource-intensive process. Moreover, the list would need to be updated and maintained on an ongoing basis. Its existence would, however, provide certainty about whether a particular country does, or does not, provide effective privacy protection, a judgment that would normally be almost impossible for an agency or organisation to make with any degree of confidence. The Commission agrees with the ALRC that the compilation of the list should be the responsibility of the Australian Government, and may be a suitable task for the Department of Prime Minister and Cabinet, in consultation with such agencies as Department of Foreign Affairs and Trade and the OPC.⁵⁴ In our view, any such list in NSW legislation should replicate the list developed by the Australian Government and should be contained in the regulations to the Act.

11.55 Attempting to minimise the effect of the “reasonable belief” test in the light of the concerns raised by stakeholders, the ALRC was of the view that “the ‘required or authorised by or under law’ exception, ... will allow agencies and organisations to transfer personal information where required or authorised by or under law to do so, thereby removing the need for them to rely on [UPP 11.1(a)] in many instances”. In the

52. For example, Korea and Taiwan have privacy legislation that does not apply to certain industries and categories of data. Similarly, Hong Kong and New Zealand have weak or non-existent protection for onward transfer of data: referred to in C Connolly, “Weak protection for offshore data – the ALRC recommendations for Cross-border Transfers” (2008) 5 (3-4) *Privacy Law Bulletin* 42, 43.

53. ALRC Report 108 vol 2 [31.210]-[31.215].

54. ALRC Report 108 vol 2 [31.217].

Commission’s view, this is all the more reason why the “reasonable belief” test is not justified and should be removed.⁵⁵

RECOMMENDATION 14

If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient who is outside of Australia and an external territory, the agency or organisation should remain accountable for that personal information unless the recipient of the information is subject to a law that effectively upholds privacy protections that are substantially similar to, or more favourable than, the protections afforded by privacy legislation in Australia and that applies in a “listed jurisdiction”. A “listed jurisdiction” is one that is specifically identified in a legislative instrument for the purposes of UPP 11.

Binding schemes

11.56 In addition to laws and contracts, UPP 11.1(a) also makes reference to a “binding scheme ... which effectively upholds privacy protections that are substantially similar to these principles [UPPs]”. NPP 9 also makes reference to “binding schemes”. Such schemes could include, for example, inter-governmental agreements or effective self-regulatory schemes. As is the case with “laws”, the Commission is of the view that such schemes should be identified in an official list.

RECOMMENDATION 15

In UPP 11 binding schemes should be dealt with in the same way as laws.

Contracts

11.57 Contracts are commonly used, and used effectively, to protect privacy in cross-border data transfers.⁵⁶ In the Commission’s view, an agency or organisation in Australia should remain accountable for the transfer of personal information to a recipient outside Australia unless the contract in question contains terms that are substantially similar to, or more favourable than, the protections afforded by Australian privacy legislation. As in the case of laws,⁵⁷ it ought not to suffice, in order to avoid such accountability, that the agency or organisation “reasonably believes” that the contract in issue provides such privacy protection.

55. ALRC Report 108 vol 2 [31.140].

56. ALRC Report 108 vol 2 [31.224]-[31.225].

57. See para 11.53-11.55.

11.58 To assist parties in determining whether or not contractual terms reach the requisite standard of privacy protection, the ALRC has recommended that the federal Privacy Commissioner should develop and provide guidance on the ‘Cross-border Data Flows’ principle (UPP 11) that, among other matters, focuses on “the issues that should be addressed as part of a contractual agreement with an overseas recipient of personal information”.⁵⁸ The Office of the Victorian Privacy Commissioner has already published *Model Terms for Cross-border Data Flows of Personal Information* that includes model clauses, with commentary, for the transfer of personal information outside Victoria.⁵⁹ In the Commission’s view, these guidelines provide the basis for the development, on a national basis, of model contractual terms dealing with the transfer of personal information to recipients outside Australia.

RECOMMENDATION 16

The “reasonable belief” test in relation to contracts should be replaced with a test that requires the contract to contain mandatory terms which incorporate privacy protections that are substantially similar to, or more favourable than, the protections afforded by privacy legislation in Australia.

Consent

11.59 The consent exception in NPP 9 merely requires that the individual consents to the transfer of information, as is the case under HPP 14. NPP 9 also permits the transfer of information where it is for the benefit of the individual and it is impracticable to gain the consent of the individual, but where the individual would consent if it were practicable.

11.60 The consent exception under UPP 11.1(b) is more restrictive in that it requires that the individual must be expressly advised of the consequences of providing consent:

[the] individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual’s personal information once transferred.

58. ALRC Report 108 vol 2 [31.230], Recommendation 31-7(c).

59. Office of the Victorian Privacy Commissioner, *Model Terms for Cross-Border Data Flows of Personal Information*, June 2006, Privacy Victoria «www.privacy.vic.gov.au» (publications – guidelines) at 28 June 2009.

11.61 In the Commission's view, this narrowing of the consent exception effectively avoids the problem of consent being given in circumstances where the individual is unaware of the consequence that the agency or organisation will no longer be accountable.

11.62 However, the general problems associated with consent as it relates to other UPPs and as discussed in the ALRC Report,⁶⁰ are imported here. Of particular relevance is the issue of whether the individual has provided "informed consent", that is, whether the individual has been sufficiently informed of the uses to which the information will be put if consent is given. In the Commission's view, if an individual is to provide consent that would remove the accountability principle from operating, it should be necessary that the individual is informed of all the intended uses, destination/s to which the information will be transferred and protections available in the destination jurisdiction/s. No doubt detailed information may not always be available with regards to the uses, but it is necessary that full disclosure be made, if known. The requirements under the openness principle extend to notifying an individual if his or her personal information may be transferred outside Australia.⁶¹

11.63 A number of submissions also suggested that consent ought to be express, not implied or "bundled", that is, bundled together without the consumer's knowledge or approval, (such as the transfer of information to a foreign jurisdiction) together with consent for other uses of the information with the consumer's knowledge (such as processing of an application). The Commission agrees with the view that such bundled consent would make it difficult "for a consumer to approve local use and oppose foreign use".⁶²

11.64 In the Commission's view, in addition to the current restrictions in UPP 11.1(b), the consent exception should require that an individual be advised of the uses to which the information will be put and destination jurisdictions to which the information will be transferred, before

60. ALRC Report 108 vol 1 Chapter 18.

61. See para 4.24.

62. C Connolly, "Commentary on the ALRC Recommendations for Cross Border Transfers" (2008), 4, paper presented at *Meeting Privacy Challenges: ALRC and NSWLRC Privacy Reviews Seminar*, Faculty of Law, UNSW, Sydney, 2 October 2008, «http://www.cyberlawcentre.org/ipp/events/symposium08/materials/4_Connolly_Paper2.pdf» at 14 September 2009.

providing express consent to the specific possibility of cross-border data flows.

RECOMMENDATION 17

UPP 11.1(b) should be amended to read as follows:

(b) the individual expressly consents to the transfer, after being expressly notified of the following:

- (i) the destination jurisdiction/s of the transfer and the likelihood of further transfers;
- (ii) the intended recipient/s;
- (iii) the intended uses (if known); and
- (iv) the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred.

“Required or authorised by or under law”

11.65 UPP 11(c) permits information to be transferred, without the accountability principle applying, if the “agency or organisation is required or authorised by or under law to transfer the personal information”. HPP 14(h) provides a similar exception when “the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law”. There is no specific reference to such an exception in NPP 9.

11.66 In DP 72, the ALRC proposed that if the ‘Cross-border Data Flows’ principle was extended to apply to agencies, then it should be subject to a law enforcement exception similar to the law enforcement exception proposed for the use and disclosure principle.

11.67 While some submissions to DP 72 supported the law enforcement exception,⁶³ there were others that argued it was too broad⁶⁴ or needed

63. Australian Direct Marketing Association, *Submission PR 543*, 21 December 2007; Medicare Australia, *Submission PR 534*, 21 December 2007 offered qualified support; Office of the Victorian Privacy Commissioner, *Submission PR 567*, 19 December 2007; Queensland Government, *Submission PR 490*, 19 December 2007; National Health and Medical Research Council, *Submission PR 397*, 7 December 2007, cited in ALRC Report 108 vol 2 [31.163].

64. Civil Liberties Australia, *Submission PR 469*, 14 December 2007; Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007, cited in ALRC Report 108 vol 2 [31.164].

further elements added to it.⁶⁵ Still others argued for a “required or authorised by law” exception instead of a law enforcement exception⁶⁶ for various reasons including that it may have unintended consequences.⁶⁷ The Commission agrees with the view expressed by still other stakeholders that mirroring the use and disclosure exception is unnecessary since the exceptions to the ‘Cross-border Data Flows’ principle are “an additional hurdle that must be crossed where an overseas transfer is involved”.⁶⁸

11.68 While there is no difficulty with this exception where an agency or organisation is “required by or under law” to transfer such information, there has been concern over the “authorised by or under law” limb of this exception.⁶⁹ The concern is that it may widen the ambit of the exception unnecessarily.

11.69 The distinction between being “required by law” and being “authorised by law”⁷⁰ is that in the former case the law in question “demands” or “necessitates” that something be done,⁷¹ whereas in the latter, the law in question permits it to be done but the person concerned has a discretion whether or not to do it. The Commission sees no reason why the exception should not apply to the latter situation. “Authorised”

65. ACT Government Department of Disability, Housing and Community Services, *Submission PR 495*, 19 December 2007; Australian Government Attorney General’s Department, *Submission PR 546*, 24 December 2007, cited in ALRC Report 108 vol 2 [31.163].

66. Australian Federal Police, *Submission PR 545*, 24 December 2007 called for an exception that allowed it to perform all its functions under the *Australian Federal Police Act 1979*; Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007; Australian Taxation Office, *Submission PR 515*, 21 December 2007; Centrelink, *Submission PR 555*, 21 December 2007, cited in ALRC Report 108 vol 2 [31.160].

67. Australian Communications and Media Authority, *Submission PR 522*, 21 December 2007, cited in ALRC Report 108 vol 2 [31.160].

68. Australian Privacy Foundation, *Submission PR 553*, 2 January 2008; Cyberspace Law and Policy Centre UNSW, *Submission PR 487*, 19 December 2007, cited in ALRC Report 108 vol 2 [31.167].

69. C Connolly, “Weak protection for offshore data – the ALRC recommendations for Cross-border Transfers” (2008) 5 (3-4) *Privacy Law Bulletin* 42, 45.

70. See NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009) para 6.4.

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

does not mean, of course, that something can be done simply because there is no law prohibiting it.⁷²

ADEQUACY OF REMEDIAL ACTION

11.70 One of the main advantages of the accountability approach, and indeed one of the reasons it was canvassed in DP 72, was because it places liability on the agency or organisation transferring the personal information. This “ensures that an individual has the ability to seek redress from someone in Australia if the recipient breaches the individual’s privacy” making it possible for the individual to approach the local regulator, “rather than have to seek protection under a foreign law, which may not provide the same level of protection as a local law”.⁷³

11.71 Although the accountability approach allows consumers to identify the regulator more easily, the damage that occurs in a foreign country is still difficult to rectify. In privacy law, remedial action, such as the removal, correction or destruction of information is crucial, and often more important than providing compensation.⁷⁴ However, as the ALRC has observed, “the ability to investigate breaches of local privacy laws in foreign countries poses particular challenges for privacy regulators”.⁷⁵

11.72 A solution to this problem is to improve and enhance Australia’s involvement in co-operative arrangements with regulators in other jurisdictions. The ALRC referred to various ongoing arrangements such as the OPC’s membership of the Asia Pacific Privacy Authorities Forum, the APEC Privacy framework and the agreement with the New Zealand Privacy Commissioner by virtue of a Memorandum of Understanding that includes sharing of information and co-operative complaint handling as well as possibly undertaking joint investigations.⁷⁶ The Commission agrees with the ALRC that seeking further opportunities for such co-operation with foreign privacy regulators would help to deal with more effective implementation of UPP 11.

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

73. ALRC DP 72 vol 2 [28.68].

74. C Connolly, “Weak protection for offshore data – the ALRC recommendations for Cross-border Transfers” (2008) 5 (3-4) *Privacy Law Bulletin* 42, 43.

75. ALRC Report 108 vol 2 [31.219].

76. ALRC Report 108 vol 2 [31.219]-[31.222].

INTERACTION WITH OTHER UPPs

11.73 UPP 11 is fundamentally about disclosure of personal information to other countries. Thus, as a first step, an agency or organisation that transfers information overseas must also comply with the other UPPs. In effect, UPP 11 should then be consistent with all other UPPs and should comply with the requirements of all other UPPs.

11.74 Thus, it is appropriate that UPP 4 includes cross-border transfers in the list of matters that must be included in a Privacy Policy. When an organisation or agency wants to transfer information overseas, it must first determine whether it complies with UPP 5, the use and disclosure principle. UPP 7, which deals with data quality and UPP 8, which deals with data security are also particularly relevant to the offshore transfer of data.

11.75 In practice therefore, the UPPs should apply to all data at all times. As much as all disclosures of personal information should be regulated by the “Use and Disclosure” principle in the first instance since the ‘Cross-border’ principle only applies to cross-border transfer of that information, so also it must be considered in the light of all other UPPs.

11.76 Given the general interaction of principles with each other, the Note to UPP 11 cross referencing UPP 11 and the use and disclosure principle (UPP 5) to each other would seem to be unnecessary and could potentially be open to misinterpretation that the only interaction required is between those two principles. On the contrary, all of the principles should be considered and should apply to all personal information.

11.77 The Commission is therefore of the view that Note 3 to UPP 5 and the Note to UPP 11 should be removed and replaced with a Note stating that agencies and organisations are subject to the requirements of all other UPPs when transferring personal information about an individual to a recipient who is outside Australia.

RECOMMENDATION 18

Note 3 to UPP 5 should be deleted and the Note to UPP 11 should be replaced with a note stating that agencies and organisations are subject to the requirements of all other principles when transferring personal information about an individual to a recipient who is outside Australia.

THE COMMISSION'S OVERALL VIEWS

11.78 On the one hand, the shift to adopting the accountability approach and limiting the exceptions to three circumstances would seem to provide greater protection to cross-border transfers. However, the above discussion raises some significant issues that limit the scope of the current UPP 11.1 and weaken its efficacy. Indeed, one view is that “UPP 11 fails to provide even a basic level of privacy protection, and undermines all of the other UPPs as a result”.⁷⁷

11.79 The Commission’s recommended modification to UPP 11 addresses the problems it has identified and the concerns raised by limiting the scope of the exceptions and clarifying the meaning of accountability. As redrafted below, the Commission is of the view that UPP 11 has the potential to provide adequate protection to individuals whose personal information is subject to the cross-border data flows principle.

11.80 In keeping with the Commission’s evaluation of the UPPs as drafted by the ALRC, the form of UPP 11 set out below is a revised model UPP. Obviously, at the time when a State or Territory adopts the UPPs into its own legislation, the UPPs will be adapted to make sense in that State or Territory context, while preserving uniformity. For example, when UPP 11 is adopted in NSW legislation the principle will deal with the transfer of information outside NSW and will reference NSW legislative instruments.

77. C Connolly, “Weak protection for offshore data – the ALRC recommendations for Cross-border Transfers” (2008) 5 (3-4) *Privacy Law Bulletin* 42, 45.

RE-DRAFTED UPP 11

11. If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless:

- (a) the recipient of the information is subject to:
 - (i) a law or binding scheme that effectively upholds privacy protections that are substantially similar to, or more favourable than, the protections afforded by privacy legislation in Australia, and that applies in a listed jurisdiction; or
 - (ii) a contract containing mandatory contract terms which incorporate privacy protections that are substantially similar to, or more favourable than, the protections afforded by privacy legislation in Australia.
- (b) the individual expressly consents to the transfer, after being expressly notified of the following:
 - (i) the destination jurisdiction/s of the transfer and the likelihood of further transfers;
 - (ii) the intended recipient/s;
 - (iii) the intended uses (if known); and
 - (iv) the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or
- (c) the agency or organisation is required by or under law to transfer the personal information.

An agency or organisation being “accountable” for personal information means:

- (a) being responsible for the acts and practices of a recipient of personal information, the subject of a cross-border transfer; and
- (b) being liable for a breach of UPP 11 if the acts and practices of the recipient would have amounted to an interference with the privacy of an individual, if done in Australia.

A “listed jurisdiction” is one that is specifically identified in a legislative instrument for the purposes of UPP 11.

Note: Agencies and organisations are also subject to the requirements of all other principles when transferring personal information about an individual to a recipient who is outside Australia.

Appendix

- Appendix A: Submissions

Appendix A: Submissions

Office of the Privacy Commissioner, 13 October 2008

Justice Health, NSW Health, 15 October 2008

NSW Commission for Children & 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

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

Department of Ageing, Disability & Home Care, 30 October 2008

Minister for Community Services, 30 October 2008

Australian Privacy Foundation, 31 October 2008

Cyberspace Law & 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

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